Konstruktion eines semi-qualitativen Risikographen für das Eisenbahnwesen

Von der
Fakultät Architektur, Bauingenieurwesen und Umweltwissenschaften
der Technischen Universität Carolo-Wilhelmina
zu Braunschweig

zur Erlangung des Grades einer
Doktoringenieurin (Dr.-Ing.)
genehmigte

Dissertation

von
Birgit Milius
geboren am 25. August 1975
aus Magdeburg

Eingereicht am 29. September 2009
Disputation am 4. Dezember 2009

Berichterstatter Prof. Dr. Jens Braband
Prof. Dr. Jörn Pachl
Prof. Dr. Ullrich Martin

2009

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Kapitel 1

Einleitung

1.1 Motivation

Jeder Mensch ist jederzeit unterschiedlichen Risiken ausgesetzt. Während manche Risiken nur bedingt kontrolliert werden können (z.B. das Risiko, krank zu werden oder das Risiko, einer Naturkatastrophe ausgesetzt zu sein) kann versucht werden, dass von technischen Systemen ausgehende Risiko zu begrenzen. Für den Bereich des Eisenbahnwesens schreibt der deutsche Gesetzgeber in EBO (1967) vor, dass *Bahnanlagen und Fahrzeuge ... so beschaffen sein* [müssen]*, dass sie den Anforderungen der Sicherheit und Ordnung genügen.* Auch auf europäischer Ebene wird eine Begrenzung des von Eisenbahnsystemen ausgehenden Risikos angestrebt. Während für bestehende Systeme ein „Bestandsschutz“ existiert, muss für neu zu entwickelnde Systeme bzw. signifikante Änderungen an Systemen gezeigt werden, dass die damit verbundene Veränderung des Risikos akzeptabel ist.

Es existieren eine Vielzahl von Methoden, mit denen das von neuen Systemen oder signifikanten Änderungen an Systemen verbundene Risiko abgeschätzt werden kann. Es kann unterschieden werden in quantitative, detaillierte Analysemethoden, die zeitaufwändig sind und für die eine Vielzahl von Informationen benötigt werden, und qualitative Methoden, deren Anwendung im Allgemeinen intuitiver ist und für die weniger Detailinformationen benötigt werden. Aufgrund der mit quantitativen Methoden verbundenen Nachteile steht zu erwarten, dass qualitative Methoden zukünftig an Bedeutung gewinnen. Die bisher angewendeten qualitativen Methoden werfen Probleme auf, die sie für eine zukünftige Anwendung nicht geeignet erscheinen lassen. Ziel der Arbeit ist es, eine ausgewählte Methode, den Risikographen, zu analysieren, seine in bisherigen Veröffentlichungen existierenden Schwierigkeiten herauszuarbeiten und in einem zweiten Schritt ein Vorgehen abzuleiten, mit dem Riskographen konstruiert werden können. Die entwickelte Vorgehensweise wird bei der Konstruktion eines Beispielrisikographen angewendet.

1.2 Vorgehen

Nach dieser allgemeinen Einleitung beginnt das zweite Kapitel mit einer grundsätzlichen Vorstellung der Risiko-Thematik. Ziel des Kapitels ist es, einen Überblick über die Thematik der Risikobeurteilung zu geben, um eine Einordnung der Aufgabenstellung in das Themengebiet zu ermöglichen. Der Schwerpunkt liegt zum einen auf der Einführung des Risikobegriffs und der Vorstellung von Randbedingungen und Einflüssen auf das Risiko und zum anderen

auf der Vorstellung der in den relevanten Dokumenten verankerten Vorgehensweisen zur Risikoermittlung und Risikoableitung. Eine Analyse der Normen und Richtlinien zeigt, dass die wesentlichen Begriffe zum Teil unterschiedlich definiert werden. Es erfolgt deshalb eine für die Arbeit gültige Begriffsdefinition.

Im dritten Kapitel wird eine Klassifikation entwickelt, die eine systematische Gruppierung von Methoden zur Risikoabschätzung[1], d.h. auch von Risikographen ermöglicht. Es wird die Methode Risikograph vorgestellt. Der Risikograph wird von anderen Methoden zur Risikoabschätzung abgegrenzt. Um aufzuzeigen, wo bestehende Risikographen Defizite haben, werden zwei aktuelle Risikographen vorgestellt und hinsichtlich ihrer Anwendbarkeit und Nachvollziehbarkeit analysiert und diskutiert. Zum Abschluss des Kapitels werden wesentliche Anforderungen an Risikographen zusammengefasst.

Im Kapitel vier werden die Arbeitsschritte der Risikographerstellung erarbeitet und diskutiert. Im Mittelpunkt steht die Zusammenstellung der zur Verfügung stehenden Optionen für eine Risikographerstellung. Das Kapitel kann als Handbuch für die Risikographkonstruktion dienen. Die Abfolge der diskutierten Arbeitsschritte orientiert sich an den Phasen des Lebenszyklusprozesses, wie er in den Normen definiert wird.

Im fünften Abschnitt erfolgt die Anwendung der im Kapitel vier erarbeiteten Grundlagen. Es wird ein Beispielrisikograph konstruiert. Dieser orientiert sich an den Randbedingungen und Anforderungen des in VDV-Richtlinie 332 vorgestellten Risikographen zur Anwendung auf Bahnsignalanlagen bei Nichtbundeseigenen Eisenbahnen.

Im anschließenden Kapitel sechs wird beispielhaft das von den Komponenten Hauptsignal und punktförmige Zugbeeinflussung ausgehende Risiko mit dem neu konstruierten Risikographen abgeschätzt und mit den in VDV 332 erzielten Ergebnissen verglichen.

[1] Grundsätzlich kann auch von Verfahren zur Risikoabschätzung gesprochen werden. Beide Begriffe, Methode und Verfahren, sind zutreffend. Im Folgenden wird in der Arbeit bei eigenen Texten stets der Begriff Methode verwendet.

Kapitel 2

Risiko und Risikoabschätzung

2.1 Einleitung

Es werden zunächst die relevanten Dokumente eingeführt. Darauffolgend wird diskutiert, was unter Risiko zu verstehen ist und welche Einflüsse zu berücksichtigen sind. Eine Aussage zum Risiko wird mittels Risikoabschätzung getroffen. Demzufolge widmet sich ein Abschnitt der Frage, was unter Risikoabschätzung zu verstehen ist, und wie sich diese in den Gesamtlebenszyklus eines Systems einordnet. Es werden die Ansätze aus den unterschiedlichen Dokumenten vorgestellt.

2.2 Relevante Dokumente

Eine Vielzahl von Dokumenten reglementieren den Umgang mit Risiko und Sicherheit. Dazu gehören beispielsweise Richtlinien, Normen, Verordnungen und Leitfäden (Guides). Es ist nicht möglich, alle relevanten Dokumente im Detail vorzustellen. Im Folgenden werden die wesentlichen, im Rahmen der Arbeit häufig zitierten Dokumente vorgestellt und ihre Bedeutung für die vorliegende Arbeit begründet.

2.2.1 ISO/IEC Guides

Grundlegende Aussagen zu den im Rahmen von Betrachtungen zum Risiko und zur Sicherheit zu verwendenden Begriffen werden in den ISO/IEC Guides 51 und 73 getroffen. Sowohl ISO (International Organization of Standardization), als auch IEC (International Electrotechnical Comission) sind Normungsgremien. In ISO/IEC (2006) wird erläutert: *ISO and IEC have come together to provide a resource of helpful advice to standards writers in the form of Guides.*

Für die vorliegende Arbeit werden die Guides 51 und 73 als besonders relevant erachtet. Deren Inhalt wird in ISO/IEC (2006) wie folgt beschrieben:

- *ISO/IEC Guide 51, Safety aspects — Guidelines for their inclusion in standards: This helps standards writers to include safety aspects in their standards. It is applicable to any safety aspect related to people, property or the environment, or a combination of one or more of these (e.g. people only; people and property; people, property and the environment). Guide 51 adopts a risk reduction approach. The complete life cycle of a product, process or service, including both the intended use and the reasonably foreseeable misuse, is dealt with.*

- *ISO/IEC Guide 73, Risk management — Vocabulary — Guidelines for use in standards: Risk management depends on the context. Where terms related to risk management are used in a standard, it is important that their meanings are understood. The aim of this Guide is to promote the coherent description of risk management activities and the use of risk management terminology. It contributes to mutual understanding amongst the members of ISO and IEC on this huge and complex subject.*

Der ISO/IEC Guide 73 wird zur Zeit überarbeitet. In relevanten Fällen wird entsprechend auf den Inhalt des Entwurfs verwiesen.

2.2.2 DIN EN 61508

Die DIN EN 61508 ist die Norm zur *Funktionalen Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme*[1]. Die Norm ist anzuwenden, wo es keine anwendungsspezifischen Ableitungen gibt. Die DIN EN 50126 bzw. DIN EN 50129 sind die bahnspezifischen Ableitungen der DIN EN 61508. Da jedoch DIN EN 50126 und DIN EN 50129 wesentlich weniger umfangreich sind als die DIN EN 61508, sollte auch diese bei einer Anwendung im Eisenbahnwesen berücksichtigt werden.

Die DIN EN 61508 besteht insgesamt aus sieben Teilen, von denen drei Teile im Rahmen der Arbeit von besonderer Relevanz sind:

- Teil 1: Allgemeine Anforderungen
- Teil 4: Begriffe und Abkürzungen
- Teil 5: Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität

Die DIN EN 61508 wurde in den vergangenen Jahren überarbeitet. Im Oktober 2008 wurden für alle Teile der Norm die europäisch abgestimmten Schluß-Entwürfe (FprEN 61508-x:2008 mit Referenzdokument IEC 61508-x:200X (65A/527/CDV)) zur Kommentierung veröffentlicht. Da der Inhalt der Entwürfe zum Teil deutlich von den aktuellen Normen abweicht, wird, wo sinnvoll und notwendig, auf den neuen Entwurfstext eingegangen. Es wird deutlich gemacht, wo dies der Fall ist.

2.2.3 DIN EN 50126/ DIN EN 50129

Bei den Normen DIN EN 50126 *Bahnanwendungen-Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltung und Sicherheit (RAMS)* und der DIN EN 50129 *Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Sicherheitsrelevante elektronische Systeme der Signaltechnik* handelt es sich um die grundlegenden Normen für Sicherheitsnachweise der Leit- und Sicherungstechnik im Eisenbahnwesen. Die in diesen Normen gemachten, normativen Aussagen müssen bei der Erstellung eines Risikographen berücksichtigt werden.

Es handelt sich bei den Normen um vom Deutschen Kommitee für Normung (DIN) übernommene, europäische Normen, die in einem europaweiten Abstimmmungsprozess erstellt und angenommen wurden.

[1] Die entsprechende englischsprachige Norm ist die IEC 61508: Functional safety of E/E/PE safety-related systems.

2.2.4 VDV-Richtlinien

Im Verband Deutscher Verkehrsunternehmen (VDV) sind die Unternehmen des öffentlichen Personennahverkehrs und des Güterverkehrs mit Schwerpunkt Eisenbahngüterverkehr in Deutschland organisiert. Eine wesentliche Aufgabe des Verbands ist die *Erarbeitung einheitlicher technischer, betrieblicher, rechtlicher und wirtschaftlicher Grundsätze mit dem Ziel einer bestmöglichen Betriebsgestaltung* (VDV (2008)).

Für die vorliegende Arbeit sind vor allem die Schriften VDV 332 *Sicherheitsintegritätsanforderungen für Bahnsignalanlagen bei Nichtbundeseigenen Eisenbahnen (NE)* und VDV 334 *SIG RZA-NE Richtlinie für die Zulassung und Abnahme von Bahnsignalanlagen bei Nichtbundeseigenen Eisenbahnen (NE)* von Bedeutung. Die Schriften des VDV sind nicht verbindlich. Für die Mitgliedsunternehmen spezifizieren und ergänzen die entsprechenden Schriften die allgemeingültigen Normen, z.B. DIN EN 61508 bzw. DIN EN 50126.

In der VDV 334 (2007) wird explizit ausgeführt: *Als eine den bestehenden Rechtsvorschriften nachgeordnete Richtlinie beschreibt die SIG RZA-NE Verfahren, mit denen die Einhaltung von Rechtsvorschriften unter Berücksichtigung von allgemein anerkannten Regeln der Technik im Anwendungsbereich nachweisbar sichergestellt wird. Hinsichtlich der erforderlichen Risikoanalyse verweist die SIG RZA-NE auf die bewährten und anerkannten Analyseverfahren der VDV-Schrift 332.*

Die VDV-Schrift 332 wurde im Juli 2008 neu herausgegegeben. Sie unterscheidet sich zum Teil von der Vorgängerversion aus dem Jahr 1997. Die VDV-Schrift 334 wurde im November 2007 veröffentlicht.

2.2.5 Verordnung über die Festlegung einer gemeinsamen Sicherheitsmethode für die Evaluierung und Bewertung von Risiken

Basierend auf die von der European Railway Agency (Europäische Eisenbahnagentur, ERA[2]) erstellte *Empfehlung zur ersten Reihe gemeinsamer Sicherheitsmethoden/ Recommendation for the 1st set of Common Safety Methods (ERA-REC-02-2007-SAF (2007))* wurde von der EU-Kommission die Verordnung über die Festlegung einer gemeinsamen Sicherheitsmethode für die Evaluierung und Bewertung von Risiken (Verordnung EG Nr. 352/ (2009)) verabschiedet.

Die Aufgabe der Verordnung wird wie folgt angegeben (Verordnung EG Nr. 352/ (2009), Artikel 1(1)): *Zweck der CSM für die Evaluierung und Bewertung von Risiken ist es, das Sicherheitsniveau im Schienenverkehr in der Gemeinschaft aufrechtzuerhalten oder — soweit erforderlich und nach vernünftigem Ermessen durchführbar — zu verbessern. Die CSM erleichtert den Zugang zum Markt für Schienenverkehrsdienste durch eine Harmonisierung*

- *der Risikomanagementverfahren, die zur Bewertung der Sicherheitsniveaus und der Erfüllung der Sicherheitsanforderungen angewandt werden;*
- *des Austauschs sicherheitsrelevanter Informationen zwischen den verschiedenen Akteuren des Eisenbahnsektors mit dem Ziel, ein Sicherheitsmanagement über die innerhalb des Sektors bestehenden verschiedenen Schnittstellen hinweg zu gewährleisten;*
- *der aus der Anwendung eines Risikomanagementverfahrens resultierenden Ergebnisse.*

Die Verordnung gilt für alle signifikanten Änderungen des Eisenbahnsystems.

[2]Es wird im Folgenden die mit der Abkürzung übereinstimmende Bezeichnung European Railway Agency verwendet.

2.2.6 Rechtliche Stellung der vorgestellten Dokumente

Es wurde gezeigt, dass eine Vielzahl von Dokumenten vorliegt, die im Rahmen des zu erstellenden Risikographen zu berücksichtigen sind bzw. beachtet werden sollten.

Grundsätzlich ist zu unterscheiden in Veröffentlichungen mit Gesetzescharakter, die unbedingt eingehalten werden müssen, und Veröffentlichungen mit empfehlendem Charakter. In Wikipedia (2009) heißt es bezüglich des Rechtscharakters von Normen: *Normen haben kraft Entstehung, Trägerschaft, Inhalt und Anwendungsbereich den Charakter von Empfehlungen, deren Beachtung jedermann freisteht. Normen an sich haben keine* [unmittelbare] *rechtliche Verbindlichkeit. Normen können durch Rechts- und Verwaltungsvorschriften eines Gesetz- oder Verordnungsgebers oder durch Verträge, in denen ihre Einhaltung vereinbart wurde, verbindlich werden.* Aus den oben vorgestellten Dokumenten entspricht lediglich die Verordnung zu den gemeinsamen Sicherheitsmethoden (Verordnung EG Nr. 352/ (2009)) einem verbindlichen Gesetz.

Bei der Anwendung von Dokumenten muss beachtet werden, wenn rechtlich verbindliche Dokumente andere, rechtlich nicht verbindliche Dokumente z.B. Normen als verbindlich festlegen. Dies ist beispielsweise der Fall bezüglich der Technical Specification of Interoperability (TSI). Bei den TSI handelt es sich um Entscheidungen der Europäischen Kommission, die als solche Gesetzescharakter haben. Innerhalb der TSI wird ggf. die Anwendung der europäischen Normen als verbindlich gefordert. Ein Beispiel dafür ist die Entscheidung 2006/679/EG (2006), in der die europäischen Normen EN 50126, EN 50128 und EN 50129 als verbindlich aufgelistet werden.

2.3 Risiko

2.3.1 Grundlagen

Definition

Der Begriff Risiko wird in den meisten einschlägigen Veröffentlichungen definiert. Im Folgenden wird, wenn möglich, auf die deutschsprachigen Versionen der entsprechenden Dokumente verwiesen. Wo notwendig, wird zusätzlich die englischsprachige Variante angegeben, da es aufgrund von differierenden Übersetzungen in den Dokumenten zu Verwirrung kommen kann.

Grundlage für die Definition des Begriffs in Normen ist die Definition aus dem ISO/IEC Guide 51: *risk is a combination of the probability of occurence of harm and the severity of that harm. harm* ist definiert als *physical injury or damage to the health of people or damage to property or the environment.* DIN IEC 61508-4 hat die gegebenen Definitionen ohne weitere Änderungen übernommen. In DIN EN 61508-4 lauten die Definitionen wie folgt: *Risiko: Kombination aus Wahrscheinlichkeit, mit der ein Schaden auftritt, und dem Ausmaß des Schadens* und *Schaden: physische Verletzung oder Schädigung der Gesundheit von Menschen, entweder direkt oder indirekt als ein Ergebnis von Schäden von Gütern oder der Umwelt.* In DIN EN 50126 (2000) wird Risiko definiert als *Die Wahrscheinlichkeit des Auftretens einer Gefahr, die einen Schaden verursacht sowie der Schweregrad des Schadens*, in DIN EN 50129 (2003) als die *Kombination aus Häufigkeit oder Wahrscheinlichkeit und den Folgen eines spezifizierten gefährlichen Ereignisses.*

Der aktuell gültige ISO/IEC Guide 73 definiert Risiko entsprechend dem Guide 51. In dem Entwurf zu einer überarbeiteten Version des Guides 73 wird ein etwas anderer Ansatz gewählt: *risk...effect of uncertainty.*

Der Begriff des Risikos ist eng verknüpft mit dem Begriff der Sicherheit. So definiert der ISO/IEC Guide 51 *safety* als *freedom of unacceptable risk*, was in IEC 61508-4 (1998) übernommen wurde. In der deutschen Version der Norm (DIN EN 61508-4 (2002)) wird *Sicherheit* beschrieben als *Freiheit von unvertretbaren Risiken*. Ähnlich lautet auch die Definition in DIN EN 50129 (2003), wo *Sicherheit* als *Freisein von nicht akzeptierbaren Risiken eines Schadens* beschrieben wird.

Betrachtungen zum Schaden

Wie die Definition aus dem ISO/IEC Guide 51 zeigt, können unterschiedliche Schadensarten zur Risikoermittlung herangezogen werden. Beispiele dafür sind Personenschaden, Sachschaden und Umweltschaden. Eine weitere Schadensart ist Imageschaden, z.B. durch schlechte Leistungserbringung. Gesunkenes Ansehen eines Unternehmens kann langfristig zu wirtschaftlichen Problemen führen. Grundsätzlich ist es möglich, über verschiedene Schadensarten hinweg einen Gesamtschaden zu berechnen. Dies macht es jedoch notwendig, einzelne Schadensarten ineinander umzurechnen, was einen Konsens über die Umrechnungsfaktoren voraussetzt.

Im Fall eines Eisenbahnunfalls ist damit zu rechnen, dass von den betroffenen Personen Schadensersatzanforderungen gestellt werden. Im Bürgerlichen Gesetzbuch (BGB), § 249 *Art und Umfang des Schadensersatzes* (BGB (2009)) heißt es:

1. *Wer zum Schadensersatz verpflichtet ist, hat den Zustand herzustellen, der bestehen würde, wenn der zum Ersatz verpflichtende Umstand nicht eingetreten wäre.*

2. *Ist wegen Verletzung einer Person oder wegen Beschädigung einer Sache Schadensersatz zu leisten, so kann der Gläubiger statt der Herstellung den dazu erforderlichen Geldbetrag verlangen. Bei der Beschädigung einer Sache schließt der nach Satz 1 erforderliche Geldbetrag die Umsatzsteuer nur mit ein, wenn und soweit sie tatsächlich angefallen ist.*

Das in dem Paragraphen beschriebene Konzept ist in der Rechtssprechung unter dem Begriff der Differenzhypothese gebräuchlich. Im Münchener Kommentar zum BGB (Säcker u. a. (2007)) heißt es: *Schaden ist jede Beeinträchtigung eines Interesses, wobei es sich um ein vermögenswertes oder um ein rein ideelles Interesse handeln kann. Bei der wertenden Erfassung des jeweiligen Vermögensgegenstands ist nicht allein sein Bestand entscheidend; zu berücksichtigen sind auch die dem Inhaber durch den Vermögensgegenstand eröffneten Verwendungsmöglichkeiten, wenn der betreffende Vermögensgegenstand seiner Funktion nach dazu bestimmt ist, dem Rechtsträger gerade diese zu schaffen und zu erhalten..*

Betrachtungen zu Rate und Wahrscheinlichkeit

Aussagen zum Eintritt eines Unfalls werden im Allgemeinen als Rate oder Wahrscheinlichkeit getroffen.

- Eine Beispiel für die Definition von Wahrscheinlichkeit ist die Definition für Wahrscheinlichkeit des Ausfalls bei Anforderung in IEC 60050-191 (1990): *probability of failure to operate* wird definiert als *probability that an item fails to operate when required. This probability is estimated by the ratio of the number of failures to operate for a given number of commands to operate, to the number of commands.*

- Ein Beispiel für die Definition von Rate ist die Definition von Ausfallrate, beispielsweise in IEC 60050-191 (1990): *(instantaneous) failure rate* wird definiert als *the limit, if it exists, of the quotient of the conditional probability that the instant of a failure of a non-repaired item falls within a given time interval and the duration of this time interval, when δ t tends to zero, given that the item has not failed up to the beginning of the time interval. An estimated value of the instantaneous failure rate can be obtained by dividing the ratio of the number of items which have failed during a given time interval to the number of non-failed items at the beginning of the time interval, by the duration of the time interval.*

Risikoermittlung

Risiko kann qualitativ und quantitativ ermittelt werden. Basis einer Risikoermittlung sollte ein Risikomodell sein, welches alle relevanten Parameter abbildet. Basierend auf den Angaben des Risikomodells und ggf. externen Vorgaben ist die Risikoart festzulegen. Dies gilt besonders, wenn im Rahmen der Risikoabschätzung Personenschaden zu berücksichtigen ist (siehe folgenden Abschnitt). Basierend auf dem entwickelten Modell kann eine Beschreibung des Risikos in Form einer mathematischen Formel erfolgen, in der die das Risiko abbildenden Parameter miteinander verknüpft werden. Ein Beispiel dafür ist die Risikoformel nach Braband, die in Abschnitt 4.8.3 näher beschrieben wird.

Individuelles und kollektives Risiko

Im Eisenbahnwesen haben Risikobeurteilungen in der Vergangenheit den zu erwartenden Personenschaden analysiert und ein individuelles Risiko ermittelt. Auch die Bestimmung eines auf eine Gruppe von Personen bezogenen Risikos (kollektives Risiko, Gesellschaftsrisiko) ist möglich. Die in DIN EN 50129 (2003) gegebenen Beispiele (z.B. bei der Darstellung des Risikoanalyseprozesses) deuten auf die Präferenz des individuellen Risikos als Betrachtungsgröße hin. In Oettli u. a. (1998) wird hingegen ausgeführt, dass aus Sicht der Allgemeinheit und auch von Unternehmen das kollektive Risiko von besonderem Interesse ist, da bei katastrophalen Ereignissen im Allgemeinen das individuelle Risiko sehr gering ist. Das niedrige individuelle Risiko trägt nach Meinung der Autoren nicht den unter Umständen bedeutenden Auswirkungen Rechnung.

In DIN EN 50129 (2003) wird individuelles Risiko definiert als *Risiko, dass nur auf ein einzelnes Individuum bezogen ist.*

Kollektives Risiko wird weder in DIN EN 50126 (2000), DIN EN 50129 (2003) noch in DIN EN 61508-4 (2002) definiert. In Kroeger (2002) heißt es, dass das kollektive Risiko ein *Risiko der gesamten oder eines Teils der Gesellschaft* ist. In Yellow Book (2002) steht das kollektive Risiko im Mittelpunkt der Risikobetrachtungen für das Eisenbahnwesen. Es wird definiert als *the average number of equivalent fatalities per year occurring on mainline railways.* Unter *equivalent fatalities* wird der Gesamtpersonenschaden unter Berücksichtigung von Leicht- und Schwerverletzten sowie Toten verstanden.

Gesellschaftliches Risiko (*societal risk*) ist ein Begriff, welcher in der europäischen Sicherheitsdirektive (Sicherheitsrichtlinie (2004)) verwendet wird. Allerdings wird der Begriff dort nicht definiert. In UIC (2002) werden verschiedene Vorschläge gemacht, was unter *societal risk* verstanden werden kann:

- *risks that affect society as a whole, such as environmental harm. This is in addition to the*

total risk of harm to individual passengers, staff, level crossing users and unauthorised persons;

- *risks to persons near the railway (railway neighbours), such as from hazardous goods;*
- *risks of collective accidents, that is of accidents causing multiple fatalities;*
- *intermodal effects, for example that passengers will transfer to road because they perceive the railway to be unsafe;*
- *the risk that the public will lose trust in the institutions of the State.*

In Yellow Book (2002) wird Gesellschaftsrisiko im Unterschied zum kollektiven Risiko definiert als *a measure of the frequency of accidents, which lead to multiple fatalities.*

Eine eindeutige Unterscheidung von kollektivem Risiko und Gesellschaftsrisiko ist schwierig. Es wird im Folgenden auf eine Nutzung des Begriffs gesellschaftliches Risiko verzichtet. Es wird unterschieden in individuelles Risiko und kollektives Risiko. In Anlehnung an die in DIN EN 50129 (2003) für das individuelle Risiko gegebene Definition wird kollektives Risiko definiert als *Risiko, dass auf eine (festgelegte) Personengruppe bezogen ist.*

2.3.2 Zulässigkeit von Risiko

Tolerierbares Risiko - Grenzrisiko

Im Zusammenhang mit Risikonachweisen wird häufig der Begriff des tolerierbaren Risikos verwendet. Dieser Begriff wird in DIN EN 50129 (2003) nicht definiert. In DIN EN 50126 wird der Begriff des *vertretbaren Risikos* eingeführt: *Der maximale Grad an Risiko durch ein Produkt, der für ein Bahnunternehmen tolerierbar ist.* In DIN EN 61508-4 (2002) wird definiert: *tolerierbares Risiko* ist *...Risiko, das basierend auf den aktuellen gesellschaftlichen Wertvorstellungen in einem gegebenen Zusammenhang tragbar ist.* In dieser Norm ist dem tolerierbaren Risiko das Grenzrisiko gegenüber gestellt: *Risiko, das vorgesehen ist, für eine spezielle Gefährdung unter Berücksichtigung des EUC-Risikos zusammen mit den sicherheitsbezogenen E/E/PE-Systemen und den anderen risikoreduzierenden Maßnahmen erreicht zu werden.*

Der Unterschied zwischen tolerierbarem Risiko und Grenzrisiko besteht darin, dass das tolerierbare Risiko subjektiv, basierend auf der Gefühlslage der Menschen in der betrachteten Gesellschaft wahrgenommen wird, wohingegen das Grenzrisiko durch Aufsichtsbehörden, im Allgemeinen basierend auf dem tolerierbare Risiko und unter Berücksichtigung der Risikoakzeptanzkriterien, festgesetzt wird. Das Grenzrisiko ist maximal gleich oder aber geringer als das tolerierbare Risiko. Die Unterscheidung in tolerierbares Risiko und Grenzrisiko ist nicht in allen Normen enthalten. Es wird im Weiteren der Begriff des tolerierbaren Risikos verwendet. Die Praxis zeigt, dass sich umgangssprachlich, unabhängig von der Definition, der Begriff des tolerierbaren Risikos eingebürgert hat.

Definition von Risikoakzeptanzkriterien

Von jedem System geht ein Risiko aus, welches im Rahmen des Risikobeurteilungsprozesses analysiert und bewertet werden muss. Für jede Risikobeurteilung muss daher ein Risikoakzeptanzkriterium festgelegt werden. Dies ist eine Forderung der DIN EN 50129 (2003). Es wird jedoch nicht definiert, was genau unter einem Risikoakzeptanzkriterium zu verstehen ist. Eine Übersicht und Diskussion der unterschiedlichen Risikoakzeptanzkriterien ALARP (As Low

As Reasonably Practicable), GAMAB (Globalement Au Moins Aussi Bon), MEM (Minimum Endogenous Mortality), MGS (Mindestens gleiche Sicherheit) und NMAU (Nicht Mehr Als Unvermeidbar) findet sich in Braband (2004) (Bild 2.1). In der Tabelle bedeutet (basierend auf den bisherigen Erfahrungen) + eine gute Erfüllung, O eine teilweise und - eine weniger befriedigende Erfüllung des Kriteriums.

Kriterium	Transparenz	Flexibilität	Anwendbarkeit	Legalität	Aufwand
ALARP	-	+	+	-	-
MGS	+	+	+	+	0
GAMAB	+	+	-	+	0
MEM	-	-	-	0	-
NMAU	0	-	0	0	+

Bild 2.1: Übersicht über die Risikoakzeptanzkriterien aus Braband (2004)

Das Risikoakzeptanzkriterium *Mindestens gleiche Sicherheit*

Aussagen zu dem in Deutschland gültigen Risikoakzeptanzkriterium *Mindestens gleiche Sicherheit* für das Eisenbahnwesen werden in der EBO (1967) gemacht. Dort steht in §2 Allgemeine Anforderungen:

1. *Bahnanlagen und Fahrzeuge müssen so beschaffen sein, dass sie den Anforderungen der Sicherheit und Ordnung genügen. Diese Anforderungen gelten als erfüllt, wenn die Bahnanlagen und Fahrzeuge den Vorschriften dieser Verordnung und, soweit diese keine ausdrücklichen Vorschriften enthält, anerkannten Regeln der Technik entsprechen.*

2. *Von den anerkannten Regeln der Technik darf abgewichen werden, wenn mindestens die gleiche Sicherheit wie bei Beachtung dieser Regeln nachgewiesen ist.*

Die Ausführungen der EBO werden in Thoma u. a. (1996) näher erläutert: *Die gleiche Sicherheit kann bestimmt werden durch den Vergleich individueller Risiken, die in einem Sicherheitssystem einerseits bei Anwendung der anerkannten Regeln der Technik, andererseits bei Vornahme anderer Sicherheitsvorkehrungen bestehen.*

In Übereinstimmung mit dem Kommentar zur EBO (Thoma u. a. (1996)) betrachteten Risikobeurteilungen im Eisenbahnwesen in der Vergangenheit häufig das individuelle Risiko, welches, wenn möglich, aus den verfügbaren Statistiken abgeleitet wurde (z.B. Risikoanalyse FFB (Braband u. a. (2001))). Dieses wurde unter Berücksichtigung des Risikoakzeptanzkriteriums *Mindestens gleiche Sicherheit* als Grenzrisiko durch die Aufsichtsbehörden festgesetzt. In Braband u. a. (2001) wird dieses Vorgehen für die Risikoanalyse FunkFahrBetrieb (FFB) begründet.

Entgegen der häufig anzutreffenden Meinung wurde für das deutsche Eisenbahnwesen noch keine Analyse basierend auf dem MEM-Kriterium (Risikoakzeptanz basierend auf dem allgemeinen, individuellen Lebensrisiko, vorgestellt z.B. in Krebs u. a. (2000)) durchgeführt.

Ansatz der European Railway Agency

Die European Railway Agency beschäftigt sich seit Jahren mit Risikoakzeptanzkriterien. Diese sind vor allem in Hinblick auf die Interoperabilität des Eisenbahnbetriebs und die gegenseitige Anerkennung von Sicherheitsnachweisen von Bedeutung.

In ERA-REC-02-2007-SAF (2007) wurde erstmals ein semi-quantitatives Risikoakzeptanzkriterium definiert, welches in Verordnung EG Nr. 352/ (2009) übernommen wurde: *Bei technischen Systemen, bei denen im Falle eines funktionellen Ausfalls von unmittelbaren katastrophalen Folgen auszugehen ist, muss das damit verbundene Risiko nicht weiter eingedämmt werden, wenn die Ausfallrate pro Betriebsstunde kleiner oder gleich* 10^{-9} *ist.* Das als RAC-TS bezeichnete Risikoakzeptanzkriterium kann als Basis für die Ableitung weiterer Grenzwerte dienen. Vor einer Anwendung besteht jedoch Bedarf nach weiterer Spezifizierung bzw. Interpretation.

RAC-TS kann als Vorbild für die Entwicklung von Risikoakzeptanzkriterien für betriebliche Vorgänge und menschliche Handlungen dienen. Grundsätzlich, so heißt es in Cassir (2008b), sind drei unterschiedliche Formulierungen für Risikoakzeptanzkriterien für betriebliche Prozesse denkbar: *Quantitative (eg based on quantitative assessment), Semi-quantitative (eg SIL levels or specified ranges of acceptable values), Qualitative (eg independent actions – requirements on training of staff etc).* In Cassir (2008b) werden die folgenden Beispiele genannt:

- *For operational procedures, where a critical error in carrying out the tasks have a credible, direct potential for catastrophic consequences, the procedure needs to controlled... (eg by a technical system, by two independent human actions, to a certain SIL Level, etc) in order for the related isolated risk to be considered acceptable.*
- *In cases where a safety critical technical system for any reason is unavailable (i.e. not in function), and the corresponding tasks have to be carried out through operational procedures relying on human actions in fallback mode, these procedures need to be controlled...*

2.4 Risikoabschätzung in den Normen

2.4.1 DIN EN 61508

Die Norm DIN EN 61508-1 (2002) definiert einen Sicherheitslebenszyklus, welcher alle Arbeitsschritte vom Systemkonzept bis hin zur Außerbetriebnahme bzw. Ausmusterung umfasst. In diesem Lebenszyklus ist die Gefährdungs- und Risikoanalyse der dritte Arbeitsschritt. Eine Analyse ist nur möglich, wenn der vorhergehende Arbeitsschritt, die Beschreibung des zu analysierenden Systems, erfolgt ist. Die auf die Gefährdungs- und Risikoanalyse folgenden Schritte im Lebenszyklus, das Ableiten von Gesamtsicherheitsanforderungen und die Zuordnung von Sicherheitsanforderungen sind für die vorliegende Arbeit relevant.

In DIN EN 61508-1 (2002) wird der zweite Schritt des Systemlebenszyklusses als Definition des Anwendungsbereichs bezeichnet. Das der Norm DIN EN 61508-1 (2002) zugrunde gelegte Systemmodell unterscheidet in *Equipment under Control (EUC)*, *EUC-Leit- oder Steuerungssystem* sowie *sicherheitsbezogene Systeme.* Das angenommene Zusammenwirken der Komponenten kann dem Modell in Bild 2.2 entnommen werden.

Die Definitionen der Komponenten wurden DIN EN 61508-4 (2002) entnommen.

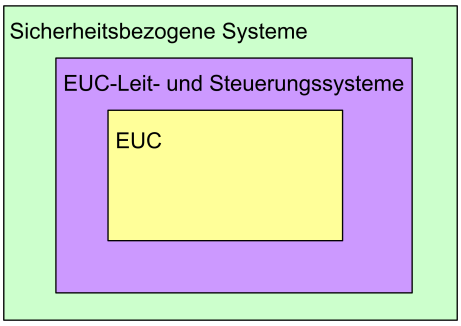

Bild 2.2: Das Systemmodell nach IEC 61508

- Unter EUC wird *Einrichtung, Maschine, Apparat oder Anlage, verwendet zur Fertigung, Stoffumformung, zum Transport, zu medizinischen oder anderen Tätigkeiten* verstanden.
- Das EUC-Steuerungssystem ist ein *System, das auf Eingangssignale der Prozesse und/-oder des Bedieners reagiert und Ausgangssignale erzeugt, die die EUC in der gewünschten Art arbeiten lässt.*
- Ein sicherheitsbezogenes System ist ein *System das sowohl die erforderlichen Sicherheitsfunktionen ausführt, die notwendig sind, um einen sicheren Zustand für die EUC zu erreichen oder aufrechtzuerhalten, als auch dazu vorgesehen ist, selbst oder mit anderen E/E/PE-sicherheitsbezogenen Systemen, sicherheitsbezogenen Systemen anderer Technologie oder externen Einrichtungen zur Risikominderung die notwendigen Sicherheitsintegrität für die geforderten Sicherheitsfunktionen zu erreichen.*

Basierend auf der Beschreibung des Anwendungsbereichs können im Rahmen der Gefährdungs- und Risikoanalyse *die Gefährdungen und gefährlichen Vorfälle der EUC und des EUC-Leit- oder Steuerungssystems* ermittelt werden. Die gemachten Aussagen (*Abschnitt 7.2.2.2: Informationen über die ermittelten Gefährdungen müssen eingeholt werden (Giftigkeit, Explosivität, Korrosivität..* und *Abschnitt 7.3.2.4: Die Art von Unfall auslösenden Ereignissen...(zum Beispiel Bauteilausfälle, Verfahrensfehler, menschliches Versagen,....)*) legen den Schluss nah, dass eine realisierungsnahe Systembeschreibung und damit auch Gefährdungsableitung erwartet wird.

Es ist das Ziel der Risikoanalyse, *die mit den...gefährlichen Vorfällen verbundenen EUC-Risiken* zu ermitteln. Explizit wird in Abschnitt 7.4.2.8 zu den anzuwendenen Methoden ausgeführt: *Die Anforderungen...können durch Anwendung entweder von qualitativen oder quantitativen Methoden der Gefährdungs- und Risikoanalyse erfüllt werden.*

Zusammenfassend wird ausgeführt, dass in der Gefährdungs- und Risikoanalyse angegeben werden muss:

- *jeder ermittelte gefährliche Vorfall und die Komponenten, die dazu beitrugen;*
- *die Auswirkungen und die Wahrscheinlichkeit der Abläufe von Ereignissen, mit denen jeder gefährliche Vorfall verbunden ist;*
- *die notwendige Risikominderung für jeden gefährlichen Vorfall;*
- ...

Für jede Gefährdung werden im vierten Schritt des Lebenszyklusses Gesamtsicherheitsanforderungen in Form von Sicherheitsfunktionen abgeleitet. Die Gesamtsicherheitsanforderungen beziehen sich auf das aus EUC und EUC-Leit- oder Steuerungssystem erwachsende Risiko. Die grundlegende Aufgabe in diesem Arbeitsschritt wird in DIN EN 61508-1 (2002) wie folgt beschrieben: *Spezifikation der gesamten Sicherheitsanforderungen für die sicherheitsbezogenen E/E/PE-Systeme, sicherheitsbezogenen Systeme anderer Technologie und externen Einrichtungen zur Risikominderung im Hinblick auf die Anforderungen zu den Sicherheitsfunktionen und den Anforderungen zur Sicherheitsintegrität.* Eine Sicherheitsfunktion ist eine *Funktion, die von einem E/E/PE-sicherheitsbezogenen System, einem sicherheitsbezogenen System anderer Technologie oder externen Einrichtungen zur Risikominderung ausgeführt wird mit dem Ziel, unter Berücksichtigung eines festgelegten gefährlichen Vorfalls einen sicheren Zustand für die EUC zu erreichen.* Sicherheitsintegrität ist die *Wahrscheinlichkeit, dass ein sicherheitsbezogenes System die geforderte Sicherheitsfunktion unter allen festgelegten Bedingungen innerhalb eines festgelegten Zeitraums anforderungsgemäß auslegt.* Es wird ausgeführt, dass die Sicherheitsanforderungen basierend auf der notwendigen Risikominderung für jeden gefährlichen Vorfall bestimmt werden müssen.

Im folgenden Schritt des Lebenszyklusses werden die Gesamtsicherheitsanforderungen auf ein oder mehrere sicherheitsbezogene Systeme (welche die Sicherheitsfunktionen ausführen) oder andere Risiko reduzierende Maßnahmen verteilt. In diesem Schritt werden basierend auf die ermittelte, notwendige Risikoreduktion den Sicherheitssystemen die Ausfallgrenzwerte und darauf basierend die Sicherheitsintegritätsanforderungen zugewiesen. Sowohl die Ausfallgrenzwerte wie auch die Sicherheitsintegritätsanforderungen beziehen sich auf Sicherheitsfunktionen. Ausschlaggebend für die Zuweisung einer Sicherheitsintegritätsanforderungen ist die notwendige Risikominderung zum Erreichen des tolerierbaren Risikos für die betrachtete Gefährdung. Diese Idee ist in Bild 2.3 verdeutlicht.

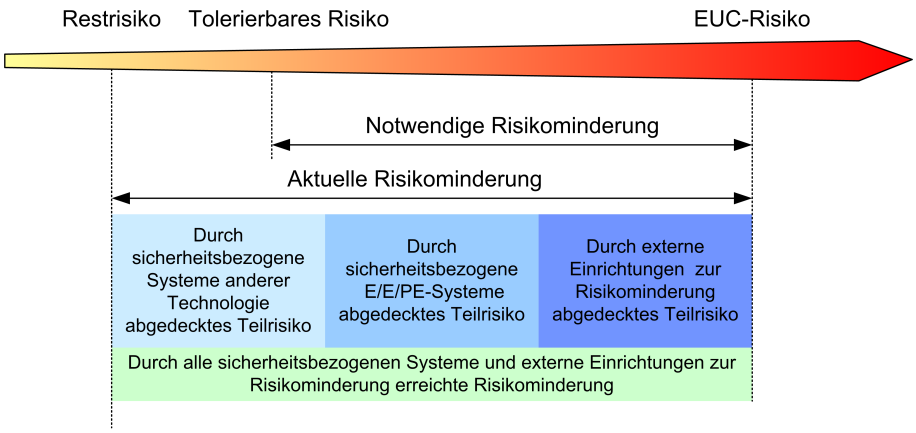

Bild 2.3: Das Konzept der Ermittlung der Sicherheitsanforderungen über den Anteil der Risikominderung nach DIN EN 61508-5

Die Norm DIN EN 61508-1 (2002) gibt in Tabellenform eine Zuordnung von Sicherheitsintegritätsleveln zu Ausfallwahrscheinlichkeiten (in Abhängigkeit der Betriebsart) vor. Tabelle 2.1 zeigt die Zuordnung für Funktionen mit hoher oder koninuierlicher Anforderungsrate. Es sei darauf hingewiesen, dass es sich bei den gegebenen Zahlenwerten um Raten handelt, nicht

Sicherheits- integritätslevel	Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung (Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde)
4	$\geq 10^{-9}$ bis $< 10^{-8}$
3	$\geq 10^{-8}$ bis $< 10^{-7}$
2	$\geq 10^{-7}$ bis $< 10^{-6}$
1	$\geq 10^{-6}$ bis $< 10^{-5}$

Tabelle 2.1: Tabelle aus DIN EN 61508-1 (2002) *Sicherheits-Integritätslevel:Ausfallgrenzwerte für eine Sicherheitsfunktion, die in der Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung betrieben wird*

(wie die Tabelle aussagt) Wahrscheinlichkeiten. Eine entsprechende Änderung wurde in FprEN 61508-1 (2008) aufgenommen.

2.4.2 FprEN 61508-1:2008/ IEC 61508-1:200X (65A/527/CDV)

Es kann an dieser Stelle nicht auf alle Veränderungen eingegangen werden, die der Normentwurf im Unterschied zur aktuellen Norm enthält. Es werden nur Aspekte erläutert, die im Rahmen der Arbeit von besonderem Interesse sind.

Der grundsätzliche Ablauf des Lebenszyklusses wurde im Normentwurf FprEN 61508-1 aus der aktuellen Norm übernommen.

In der aktuellen Norm DIN EN 61508-1 (2002) ist die wesentliche Leitgröße für alle Maßnahmen bezüglich der Tolerabilität von Risiko, der Festsetzung von Anforderungen und der Zuweisung von Sicherheitsintegritätsanforderungen die notwendige Risikominderung. Dieses Konzept ist aus Sicht des DIN EN 61508-Systemmodells nachvollziehbar, da in diesem Konzept die Risikominderung durch separate Systemteile nachzuweisen war. Für andere Industriezweige, in denen eine Trennung der Systemkomponenten in Leit- und Steuerungssysteme und Sicherheitssysteme nicht möglich ist, war die Erfüllung der Normanforderungen schwierig. Dies gilt auch für Situationen, in denen dem EUC bzw. EUC-Leit- oder Steuerungssystem eine so niedrige Ausfallrate zuzuweisen war, dass dies die Zuweisung und Einhaltung einer Sicherheitsintegritätsanforderung notwendig machte.

In dem vorliegenden Entwurf wurde Abstand genommen von einer ausschließlichen Betrachtung der Risikominderung. Auch wurde die Möglichkeit von EUC-Leit- und Steuerungssystemen mit niedriger Ausfallrate berücksichtigt. In Abschnitt 7.5.2.4. bzw. 7.5.2.5. heißt es explizit: *The overall safety integrity requirements shall be specified in terms of either*

- *the risk reduction required to achieve the tolerable risk, or*
- *the tolerable hazardous event rate so as to meet the tolerable risk.*

If, in assessing the EUC risk, the rate of dangerous failure of the EUC control system is claimed as being lower than 10^{-5} *dangerous failures per hour then the EUC control system shall be considered to be a safety-related system subject to the requirements of this standard.*

2.4.3 DIN EN 50126

Auch die DIN EN 50126 (2000) definiert einen Lebenszyklusprozess mit den Phasen Systemdefinition und Anwendungsvoraussetzungen, Risikoanalyse und Ableitung von Sicherheitsanforderungen.

Es werden in der Norm detailliert Informationen gegeben, welche Aspekte bei der Systemdefinition und dem Aufstellen der Anwendungsvoraussetzungen/-bedingungen zu berücksichtigen sind.

Im Rahmen der Risikoanalyse sind die Gefahren und die zugehörigen, auslösenden Ereignisse zu identifizieren und die mit den Gefahren verbundenen Risiken zu ermitteln. Eine funktionale Gefahrenbetrachtung wird nicht gefordert. Vielmehr lassen die detaillierten Hinweise auf die zu berücksichtigenden Einflüsse (z.B. Berufserkrankungen, Systemmissbrauch, natürliche Umfeldbedingungen) den Schluss zu, dass eine realisierungsnahe Gefahrenidentifikation erwartet wird. Laut Norm sind ein Risikomanagementprozess zu erstellen und Aussagen zur Zulässigkeit des Risikos zu treffen. Es werden beispielhafte Tabellen (z.B. Kategorisierung der Häufigkeit von Gefahrenfällen, Kategorisierung von Gefahrenstufen) für eine qualitative Beurteilung der Gefahren zur Verfügung gestellt, welche von den Bahnunternehmen vor einer Anwendung anzupassen sind.

Aufgabe in der darauffolgenden Phase ist es, *funktionale Anforderungen und unterstützende Leistungsanforderungen einschließlich sicherheitsrelevanter funktionaler Anforderungen und Anforderungen für die Safety Integrity jeder Sicherheitsfunktion* festzulegen. Safety Integrity ist: *Die Wahrscheinlichkeit dafür, dass ein System die festgelegten Sicherheitsanforderungen unter allen festgelegten Bedingungen innerhalb einer bestimmten Zeitspanne erfüllt.* Im Begleittext wird ausgeführt, dass Safety Integrity nur für Sicherheitsfunktionen spezifiziert werden kann. Es wird jedoch nicht definiert, was eine Sicherheitsfunktion ist. Da es auch keine Aussagen zum der Norm zugrunde liegenden Systemmodell gibt, wird nicht klar, wie System und (Sicherheits-)Funktion zusammenhängen.

2.4.4 DIN EN 50129

Die Norm DIN EN 50129 (2003) beschäftigt sich schwerpunktmäßig mit dem Prozess des Sicherheitsnachweises und dessen Möglichkeiten. Darüber hinaus enthält die Norm mehrere normative Anhänge, von denen der Anhang A für die vorliegende Arbeit relevant ist.

Die Aufgabe des Anhangs A wird wie folgt beschrieben: *Dieser Anhang liefert Einzelheiten zur Ableitung, Zuteilung und Verwirklichung von Sicherheitsanforderungen und Sicherheitsintegrität sowie zur Anwendung der Sicherheitsanforderungsstufen in sicherheitsrelevanten Systemen für Eisenbahnanwendungen.* Es wird eine Methodik zur Ableitung der Sicherheitsanforderungen vorgestellt, in deren Zentrum eine definierte Schnittstelle der Prozesse der Eisenbahnverwaltung (Risikoanalyse) auf der einen Seite und des Herstellers (Gefährdungsbeherrschung) auf der anderen Seite steht. Die Darstellung dieses Zusammenhangs erfolgt in Form einer Sanduhr (Bild 2.4). Im englischen Sprachraum ist die Darstellung als sogenanntes Bow-Tie-Modell (gedrehte Sanduhr) üblich.

Für die Arbeit relevant ist der obere Teil der Sanduhr, die sogenannte Risikoanalyse. Die dort genannten Arbeitsschritte entsprechen weitgehend den Phasen des Lebenszyklusprozesses aus DIN EN 50126 (2000) und DIN EN 61508-1 (2002).

Die ersten beiden Schritte des Risikoanalysseprozesses sind Systemdefinition und Gefährdungsidentifikation. Eine umfassende und hinreichende Systemdefinition ist Voraussetzung für

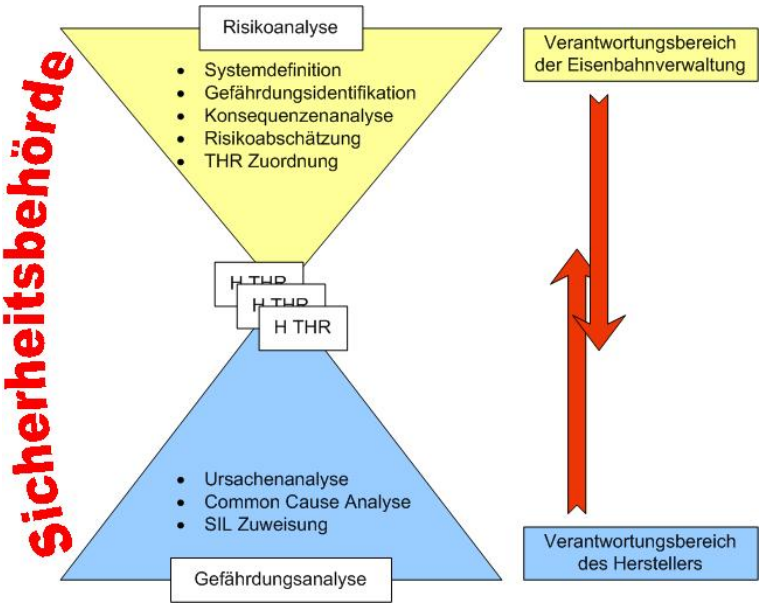

Bild 2.4: Das Sanduhrmodell in DIN EN 50129 (2003)

eine erfolgreiche Risikoanalyse.

Die Norm führt aus, dass zur Gefährdungsidentifikation unterschiedliche Vorgehensweisen gewählt werden können. Hervorzuheben ist, dass die Norm feststellt, dass Gefährdungen realisierungsunabhängig zu ermitteln sind, was im Allgemeinen als funktional zu definieren verstanden wird: *Es liegt in der Verantwortung der Eisenbahnverwaltung das System zu definieren (unabhängig von der technischen Realisierung), die zu dem System relevanten Gefährdungen zu identifizieren.*

Bezüglich Folgenanalyse, Riskoabschätzung und Zuordnung der tolerierbaren Gefährdungsraten heißt es in DIN EN 50129 (2003):
Es liegt in der Verantwortung der Eisenbahnverwaltung:

- *die Folgen, d. h. die Verluste, zu analysieren,*
- *die Risikoakzeptanzkriterien zu definieren,*
- *die tolerierbaren Gefährdungsraten abzuleiten und*
- *sicherzustellen, dass das sich ergebende Risiko tolerierbar ist (in Bezug auf geeignete Risikoakzeptanzkriterien).*

Die alleinige Forderung ist, dass die tolerierbaren Gefährdungsraten unter Berücksichtigung der Risikoakzeptanzkriterien abgeleitet werden müssen. Die Risikoakzeptanzkriterien sind nicht durch diese Norm festgelegt, sondern sie sind abhängig von nationalen oder europäischen gesetzlichen Anforderungen.
Die Analysemethoden müssen entweder

- *das resultierende (individuelle) Risiko explizit abschätzen, oder*
- *die tolerierbaren Gefährdungsraten über einen Vergleich mit der Leistungsfähigkeit existierender Systeme oder von anerkannten Regeln der Technik mittels statistischer oder analytischer Methoden ableiten, oder*

- *die tolerierbaren Gefährdungsraten aus alternativen qualitativen Verfahren ableiten, falls sie als Ergebnis eine Liste von Gefährdungen und zugehörigen THR festlegen.*

Basierend auf den tolerierbaren Gefährdungsraten können die Sicherheitsintegritätsanforderungen für das System, Teilsysteme und ggf. Elemente festgelegt werden.

Bei der Beschreibung des Risikoanalyseprozesses wird nicht der Bogen zu den Sicherheitsfunktionen geschlagen. Auch wird dieser Begriff nicht definiert. Bei der Erläuterung zum Ableiten der Sicherheitsanforderungsstufen wird ausgeführt, dass die Sicherheitsanforderungsstufen den sicherheitsrelevanten Funktionen zugeordnet werden (und diese wiederum in Teilsystemen verwirklicht werden). Der Begriff der sicherheitsrelevanten Funktion wird in der Norm nicht definiert. Durch eine Kombination der Aussagen zu Sicherheit, sicherheitsrelevant und Funktion können sicherheitsrelevante Funktionen als Funktionen bezeichnet werden, die durch Aktionen oder Tätigkeiten dazu beitragen, dass ein System frei ist von nicht akzeptierbaren Risiken eines Schadens. Dies ist im Unterschied zu sehen zu der Definition von Funktion als *Art von Aktion oder Tätigkeit, durch die ein Produkt seinen beabsichtigten Zweck erfüllt.*

2.4.5 Verordnung über die Festlegung einer gemeinsamen Sicherheitsmethode für die Evaluierung und Bewertung von Risiken

In Verordnung EG Nr. 352/ (2009) wird ein Risikomanagementverfahren beschrieben, in welches ein Risikobewertungsverfahren eingebunden ist (Bild 2.5). Das Risikobewertungsverfahren umfasst die Arbeitsschritte Systemdefinition, Risikoanalyse einschließlich Gefährdungsermittlung und Risikoevaluierung. Im Rahmen der Systemdefinition ist festzuhalten

a) Zweckbestimmung des Systems, z. B. vorgesehene Verwendung;

b) Funktionen und Bestandteile des Systems, sofern relevant (einschließlich z. B. menschlicher, technischer und betrieblicher Komponenten);

c) Systemgrenzen, einschließlich anderer, interagierender Systeme;

d) physische Schnittstellen (interagierende Systeme) und funktionale (Ein- und Ausgabe-) Schnittstellen;

e) Systemumgebung (z. B. Energie- und Wärmefluss, Erschütterungen, Vibrationen, elektromagnetische Beeinflussung, betriebliche Verwendung);

f) bestehende Sicherheitsmaßnahmen und — nach mehrfacher Anwendung — Definition der im Rahmen des Risikobewertungsverfahrens ermittelten Sicherheitsanforderungen;

g) Annahmen, die die Grenzen der Risikobewertung bestimmen.

Im Rahmen der Risikoanalyse sind zunächst die Gefährdungen zu ermitteln. Es ist die Vertretbarkeit des von ihnen ausgehenden Risikos anhand einem von drei genannten Grundsätze der Risikoakzeptanz zu evaluieren:

a) Anwendung der anerkannten Regeln der Technik (Abschnitt 2.3);

b) Vergleich mit ähnlichen Systemen (Abschnitt 2.4);

c) explizite Risikoabschätzung (Abschnitt 2.5).

In Übereinstimmung mit dem allgemeinen Grundsatz gemäß Abschnitt 1.1.5 sieht die Bewertungsstelle davon ab, dem Vorschlagenden Auflagen bezüglich des anzuwendenden Grundsatzes der Risikoakzeptanz zu machen.

Im ersten Fall kann eine detaillierte Risikoabschätzung entfallen. Die Risikoakzeptanz kann gezeigt werden, indem die Einhaltung der entsprechenden Regeln der Technik nachgewiesen wird. Der zweite Fall kann dann angewendet werden, wenn durch ein neues System ein altes,

existierendes System ersetzt werden soll. In beiden Fällen muss der Nachweis gefährdungsspezifisch erfolgen. Für eine Risikoabschätzungsmethode ist das im dritten Anstrich vorgestellte Vorgehen anzuwenden und der Kalibrierung der Methode zugrunde zu legen. Es heißt in Verordnung EG Nr. 352/ (2009): *Die explizite Risikoabschätzung und -evaluierung muss mindestens folgende Anforderungen erfüllen:*

a) Die für die explizite Risikoabschätzung eingesetzten Methoden geben das System, das der Bewertung unterzogen wird, und seine Parameter (einschließlich aller Betriebsmodi) korrekt wieder.

b) Die Ergebnisse sind ausreichend präzise, um als solide Entscheidungshilfe dienen zu können. Das bedeutet, dass geringfügige Änderungen bei den zugrunde gelegten Annahmen oder Voraussetzungen nicht zu erheblich unterschiedlichen Anforderungen führen dürfen.

2.4.6 MISRA Guidelines for the Safety Analysis

MISRA, the Motor Industry Software Reliability Association, hat in Misra (2005) den Prozess der Sicherheitsanalyse für das Automobilwesen beschrieben. Das zugrunde liegende Systemmodell wird in Jesty u. a. (2006) erläutert. Das Automobilwesen ist in vielen Aspekten dem Eisenbahnwesen ähnlicher als die Prozessindustrie, aus der heraus die DIN EN 61508-1 (2002) entstanden ist. Aus diesem Grund wird an dieser Stelle die Argumentation von Jesty für ein von der DIN EN 61508-1 (2002) abweichendes Vorgehen gegeben.

In Jesty u. a. (2006) beschäftigt sich Jesty mit der Anwendbarkeit der DIN EN 61508-1 (2002) im Automobilwesen. Als wesentliches Problem führt er aus, dass *. . . there are no hazards associated with normal driving and hence there is no risk associated with the EUC (vehicle).* Dies widerspricht der Grundidee des in DIN EN 61508-1 (2002) zugrunde gelegten Vorgehens. Jesty definiert Risiko basierend auf infolge von Fehlern des Leit- und Steuerungssystems resultierenden Unfällen (Bild 2.6).

Für das Automobilwesen kommt Jesty zu dem Fazit, dass als Grundlage für die Ableitung von Sicherheitsanforderungen die Ermittlung der notwendigen Risikoreduktion durch die Sicherheitsfunktion oder einer zulässigen Ausfallrate der Sicherheitsfunktion nicht sinnvoll ist. Stattdessen schlägt er vor, Anforderungen an die zulässige Gefährdungsrate für die betrachtete Gefährdung (nicht für eine Sicherheitsfunktion!) zu setzen. Diese Idee wird auch in dem Normentwurf FprEN 61508-1 (2008) aufgenommen.

2.4.7 VDV 334: Richtlinie für die Zulassung und Abnahme von Bahnsignalanlagen bei Nichtbundeseigenen Eisenbahnen

Die VDV-Richtlinie 334 beruft sich auf den Lebenszyklusprozess nach DIN EN 50126 (2000) und DIN EN 50129 (2003).

Im Rahmen der Phase 1 erfolgt die Erstellung des Konzepts. Es werden Beispiele gegeben, was unter Systemen zu verstehen ist. Es ist offensichtlich, dass die aufgeführten Systeme auf unterschiedlichen Ebenen im Gesamtsystem Bahn liegen, d.h. jeweils einem unterschiedlichen Detaillierungsgrad entsprechen.

Es obliegt dem Bahnunternehmen, die Anlage (System im Sinne der DIN EN 50126) mit den Rahmenbedingungen und seinen Grenzen zu definieren (siehe hierzu 2.4). Systeme (im Sinne der DIN EN 50126) können sein:

- *Betriebsleit- und Zugsicherungssystem als Gesamtsystem*

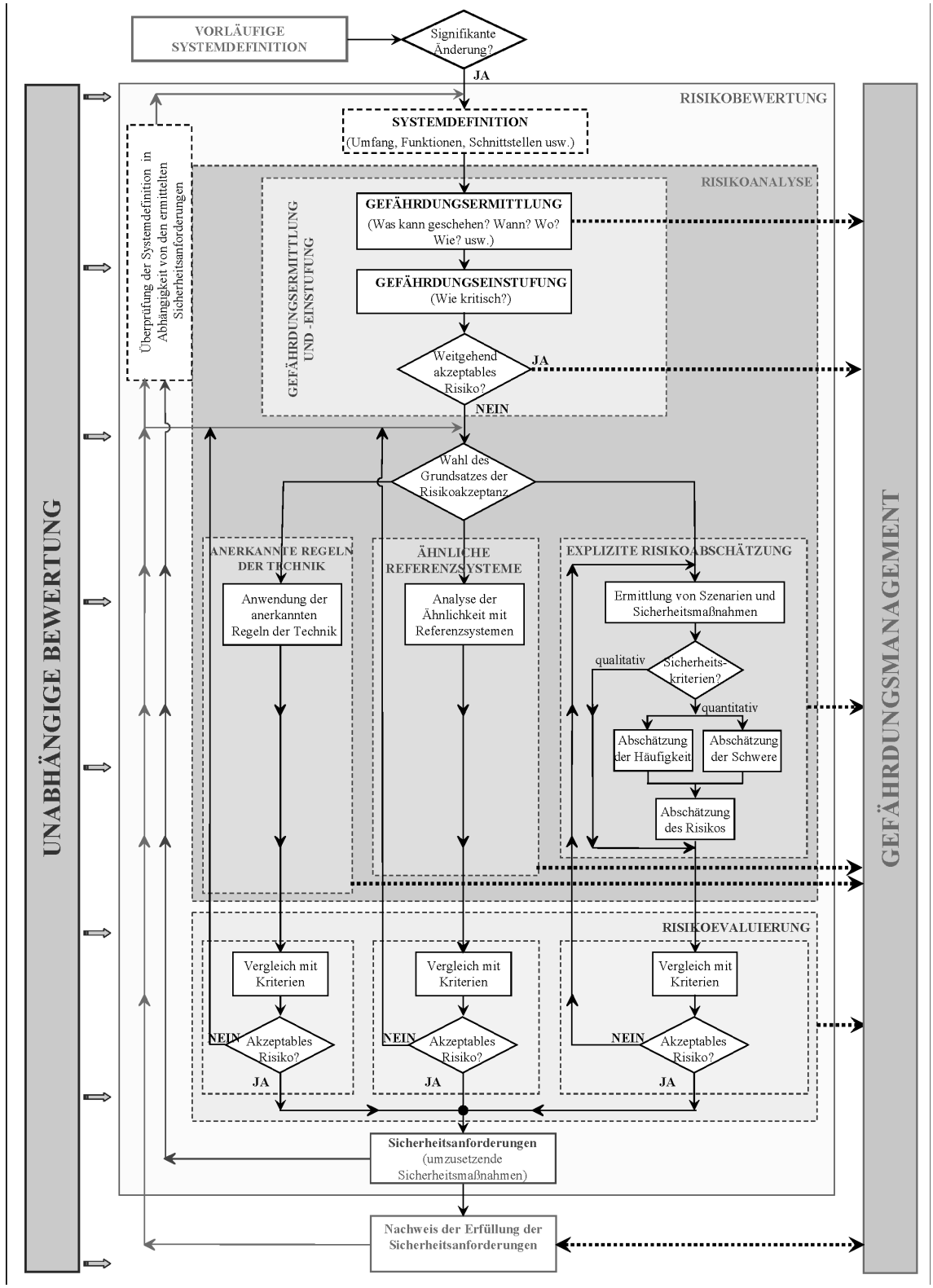

Bild 2.5: Die Risikobewertung nach Verordnung EG Nr. 352/ (2009), entnommen aus Verordnung EG Nr. 352/ (2009)

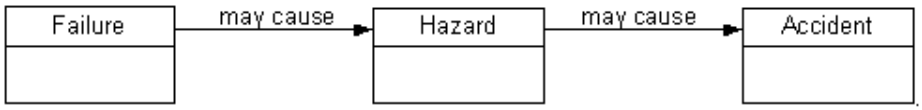

Bild 2.6: Das Entity-Relationship-Diagramm als Grundlage für das Risikomodell in Jesty u. a. (2006)

- *Zugsicherungssystem einschl. Stellwerk, Zugbeeinflussung und Bahnübergänge als Gesamtsystem*
- *Stellwerk*
- *Einzelweichensteuerung*

Im Rahmen der Systemdefinition wird ausgeführt, dass es dem Bahnunternehmen obliegt, die funktionalen, betrieblichen und technischen Anforderungen zu definieren. Da in diesem Zusammenhang die Erstellung von sicherungstechnischen Lageplänen und Gleisfreimelde-Weichen-, Signal- und Fahrstraßentabellen gefordert wird, ist zu prüfen, wie dies in Übereinstimmung mit der von DIN EN 50129 geforderten realisierungsunabhängigen Systembeschreibung steht.

Es heißt in VDV 334 weiter:

Die Durchführung der Risikoanalyse dient zur Ermittlung der

- *Gefährdungsidentifikation*
- *erforderlichen Ausstattungsmerkmale und Sicherheitsfunktionen sowie der*
- *ihnen zugeordneten Sicherheitsintegritätsanforderungen.*

Jedoch muss nicht für jedes System eine Risikoanalyse durchgeführt werden. Es heißt: *Zu Beginn der Risikoanalyse ist in einem vereinfachten Verfahren durch den Betreiber festzustellen, ob es sich um ein System von sicherheitstechnisch untergeordneter Bedeutung handelt. In diesem Fall kann im Einvernehmen mit der Aufsichtsbehörde von den sicherheitsbezogenen Aktivitäten im Zulassungs- und Abnahmeprozesses abgesehen werden.* Es wird nicht dargelegt, was unter einem System mit *sicherheitstechnisch untergeordneter Bedeutung* zu verstehen ist.

Es werden drei Vorgehensweisen zur Ableitung der Sicherheitsanforderungen unterschieden:

- Übernahme projektunabhängiger Sicherheitsintegritätsanforderungen aus der VDV-Schrift 332,
- Durchführen einer qualitativen Risikoanalyse nach den Grundsätzen der VDV-Schrift 332,
- Anwendung einer anderen, zur DIN EN 50126 konformen Methode der Risikoanalyse.

Zu der dritten Vorgehensmöglichkeit wird ausgeführt:

Alternativ zu den Methoden A und B können andere qualitative Methoden der Risikoanalyse gemäß DIN EN 50126 angewandt werden, ebenso Methoden, die Tolerable Hazard Rates (THR) ermitteln, wie in DIN EN 50129 (Anhang A) beschrieben.

Bei der Anwendung quantitativer Verfahren ist zu beachten, dass die erforderliche statistische Datenbasis (Gefährdungen, betriebliche Abläufe) vorhanden sein muss und das quantitative Risikoakzeptanzkriterium durch das Bahnunternehmen festzulegen und durch die zuständige Aufsichtsbehörde zu genehmigen ist (Anmerkung: Diese Datenbasis ist bisher im Geltungsbereich dieser Richtlinie nicht verfügbar).

Diese Aussagen scheinen deutlich machen zu wollen, dass eine quantitative Risikoananlyse zwar grundsätzlich möglich, aber nicht anzustreben ist.

2.5 Begriffe

Die für die Analyse von Risiko verwendeten Begriffe differieren in den unterschiedlichen Dokumenten. Dies kann zu Missverständnissen führen. In der vorliegenden Arbeit wurden bisher die Begriffe *Risikobeurteilung* für den Gesamtprozess von der Systemdefinition bis zur Zuweisung der Sicherheitsanforderungen, und *Risikoabschätzung* für den Prozess der tatsächlichen Risikoermittlung verwendet. In Bild 2.7 sind die für diese Arbeit relevanten Begriffe aus DIN EN 61508-4 (2002), DIN EN 50126 (2000), DIN EN 50129 (2003) und Verordnung EG Nr. 352/ (2009) gegenübergestellt. Die VDV-Schrift 334 bezieht sich auf DIN EN 50126 (2000) und DIN EN 50129 (2003) und wird daher nicht betrachtet.

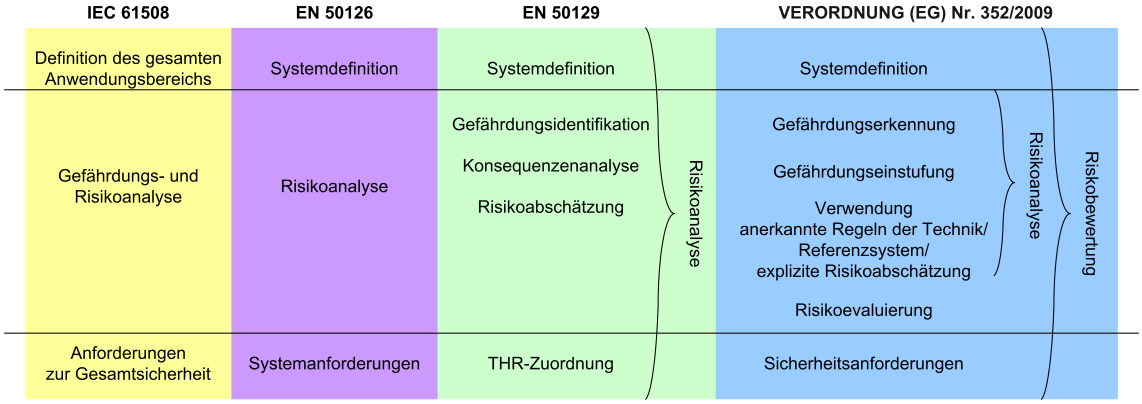

Bild 2.7: Begriffsverwendung

In dieser Arbeit werden die Arbeitsschritte für die Durchführung einer Risikobeurteilung wie folgt bezeichnet:

- Systemdefinition,
- Gefährdungsidentifikation,
- Risikoabschätzung, bestehend aus der Betrachtung der Ereignisabläufe ausgehend von der Gefährdung hin zum Unfall sowie Abschätzung des von der Gefährdung ausgehenden Risikos (Konsequenzenanalyse und Risikoabschätzung nach DIN EN 50129 (2003)),
- Ableiten von Sicherheitsanforderungen.

Kapitel 3

Der Risikograph - Stand der Technik

3.1 Klassifikation von Methoden zur Risikoabschätzung

3.1.1 Motivation

Nach erfolgreicher Systemdefinition und Gefährdungsidentifikation muss die Risikoabschätzung durchgeführt werden. Es gibt eine Vielzahl von Methoden, die angewendet werden können. DIN EN 61508-1 (2002) unterscheidet zwischen qualitativen und quantitativen Methoden zur Risikoabschätzung. Die Begriffe werden jedoch nicht definiert, sondern lediglich durch Beispiele illustriert. Auch in der Literatur wird häufig zwischen qualitativen, quantitativen, semi-qualitativen und semi-quantitativen Methoden unterschieden, ohne dass die hinter diesen Begriffen stehenden Methoden klar voneinander abgegrenzt sind.

Ziel ist es, eine strukturierte Klassifikation für Methoden zur Risikoabschätzung vorzugeben. Mindestens drei Gründe sprechen für eine nachvollziehbare, einheitliche Klassifikation dieser Methoden:

- Ohne eine klare Definition der Begriffe wie z.B. qualitativ und quantitativ kann es zu Missverständnissen kommen.
- Die Zahl von Methoden zur Risikoabschätzung ist sehr groß. Dies macht es für einen Anwender schwierig, die zu den Anforderungen der Analyse passenden Methoden herauszufinden. Eine Klassifikation anhand relevanter, nachvollziehbarer Kriterien hilft dem Anwender, zügig die Gruppe der in Frage kommenden Methoden zu identifizieren.
- Eine Klassifikation kann helfen, die Bereiche zu identifizieren, die noch nicht ausreichend durch die Forschung erarbeitet wurden.

Details der Klassifikationsableitung können Milius (2008) entnommen werden. An dieser Stelle werden die gewählten drei Klassifikationskriterien kurz vorgestellt und die abgeleitete Klassifikation angegeben.

3.1.2 Kriterien

Die vorgestellte Klassifikation wurde unter Beachtung von Nutzeranforderungen erstellt. Es wurden Kriterien gewählt, die vom Nutzer einfach zu verstehen, möglichst offensichtlich und gut überprüfbar sind. Nur wenn die gewählten Kriterien für den Anwender nachvollziehbar sind, wird dieser auf die Klassifikation zurückgreifen. Folgende Aspekte wurden als Leitlinien

für die Identifikation von Klassifikationskriterien herausgearbeitet. Dabei wurde berücksichtigt, dass zwei unterschiedliche Anwendersichtweisen unterschieden werden müssen: Anwender, die mit Hilfe der Klassifikation eine geeignete Methode auswählen wollen, und Anwender, die eine bestehende Methode in die Klassifikation einfügen wollen.

- Das Kriterium sollte möglichst kurz und knapp bewertet werden können. Kriterien, die nicht zu eindeutigen Beurteilungen führen, sind ungeeignet.
- Das Kriterium sollte möglichst viel Aussagekraft haben, d.h. möglichst viele Informationen über die Risikoabschätzungsmethode liefern.
- Damit ein Anwender eine Methode richtig klassifizieren kann, sollten die für die Klassifikationskriterien benötigten Informationen verfügbar sein.

Um die Übersichtlichkeit der Klassifikation zu gewährleisten, sollten nicht mehr als fünf Kriterien gewählt werden. Es wurden die Kriterien Parameterbeurteilung, Modell der Methode und Art des Ergebnisses - Risikoakzeptanz ausgewählt.

3.1.3 Parameterbeurteilung

Grundsätzlich können zwei Vorgehensweisen unterschieden werden. Im ersten Fall erfolgt eine Beurteilung der Parameter auf einer kontinuierlichen Skala, d.h. der anzunehmende Wert kann im Rahmen der Parameterdefinition mit beliebiger Genauigkeit frei gewählt werden. Diese Art der Parameterbeurteilung wird als quantitativ bezeichnet. Im zweiten Fall werden zu jedem Parameter Parameterklassen vorgegeben. Der Anwender kann zwar den Parameter beliebig genau schätzen, muss aber für die Risikoabschätzung entsprechend seiner Schätzung eine passende Parameterklasse wählen. Da zur Bildung der Klassen u.a. qualitative Überlegungen notwendig sind, wird diese Art der Parameterbeurteilung als qualitativ bezeichnet.

Das Kriterium Parameterbeurteilung wurde als Klassifikationskriterium gewählt, weil es einfach zu beurteilen ist. Es ist offensichtlich, ob die Parameterbeurteilung quantitativ, d.h. auf einer kontinuierlichen Skala erfolgt, oder qualitativ ist, d.h. durch Wahl einer geeigneten Klasse geschieht. Hinzu kommt, dass das Kriterium dem Anwender bereits erste Informationen über die notwendige Informationsdichte für die Analyse liefert. Es kann davon ausgegangen werden, dass für quantitative Parameterbeurteilungen die Daten genauer sein müssen, als dies für qualitative Methoden der Fall ist.

3.1.4 Modell der Methode

Eine Methode kann entweder basierend auf einem mathematischen Modell konstruiert oder durch Experten basierend auf Intuition und Erfahrung kombiniert werden. Die Art der Herleitung ist unabhängig von der Aufbereitung bzw. Darstellung der Methode für den Anwender. Methoden basierend auf einem mathematischen Modell haben den Vorteil, dass der Zusammenhang der einzelnen Parameter sowie der Beitrag der Parameter zum Risiko rechnerisch gezeigt werden kann. Es ist möglich, die Richtigkeit der ermittelten Ergebnisse quantitativ zu prüfen. Im zweiten Fall kann nicht bewiesen werden, ob die Methode zu richtigen Ergebnissen führt. Durch Vergleich mit bereits durchgeführten Analysen kann lediglich gezeigt werden, dass bei Anwendung der konstruierten Methode vergleichbare Ergebnisse ermittelt werden. Basierend auf der Beurteilung von vergleichbaren Einzelfällen wird eine Aussage zur generellen Anwendbarkeit der Methode getroffen.

Der Vorteil des Kriteriums liegt in der Tatsache, dass dem Anwender wesentliche Informationen zur Nachvollziehbarkeit und Prüfung der Analyseergebnisse gegeben werden. Dies ist besonders wichtig, wenn die Analyse durch Aufsichtsbehörden geprüft wird und diese Behörden den Nachweis für die Richtigkeit der Methode benötigen. Nachteilig ist, dass das Kriterium durch einen Anwender schwierig zu beurteilen ist, da die benötigten Informationen unter Umständen nicht zur Verfügung stehen. Es wird unterschieden in mathematisch fundierte Methoden und intuitive Methoden.

3.1.5 Art des Ergebnisses - Risikoakzeptanz

Bei jeder Methode zur Risikoabschätzung wird das von der betrachteten Gefährdung ausgehende Risiko abgeschätzt. Daraus können die folgenden Ergebnisvarianten abgeleitet werden:

Das Ergebnis ist ein Risiko, ausgedrückt beispielsweise in Opfer pro Jahr oder Stunde. Dieses Risiko kann als Eingangsgröße für weitere Betrachtungen genutzt werden. Im Besonderen ist ein expliziter Vergleich mit einem als tolerierbar angenommenen Risiko (ggf. nach Umrechnung, um vergleichbare Einheiten zu erhalten) möglich.

Das Ergebnis der Risikoabschätzung ist ein Risikokennwert. Der Risikokennwert hat im Allgemeinen nur im Kontext der Methode Aussagekraft. Für sich allein gestellt kann der Risikokennwert nicht verwendet werden; ein Vergleich mit einem Risiko ist nicht möglich. Allerdings ist ein Vergleich verschiedener, unter gleichen Randbedingungen mit der gleichen Methode ermittelter Risikokennwerte oder mit vorab (z.B. unter Berücksichtigung eines tolerierbaren Risikos) vereinbarten Risikobenchmarks möglich.

Eine dritte Möglichkeit besteht darin, dass die Methode das von einer Gefährdung ausgehende Risiko implizit mit einem tolerierbaren Risiko vergleicht. Methoden dieser Gruppe ermitteln zunächst das zu bewertende Risiko, ohne es jedoch auszugeben. Das ermittelte Risiko wird dann mit einem in der Methode hinterlegten, tolerierbaren Risiko verglichen, d.h. es erfolgt ein impliziter Risikovergleich. Darauf basierend kann beispielsweise eine zulässige tolerierbare Gefährdungsrate oder eine Risikoklasse abgeleitet werden.

Als drittes und letztes Kriterium wurde die Risikoakzeptanz bzw. die Tolerierbarkeit des Ergebnisses gewählt. Dieses Kriterium gibt dem Anwender Informationen, inwieweit eine Weiterverarbeitung des Ergebnisses notwendig und möglich ist bzw. welche Informationen bereits in der Methode implementiert sind. Hinzu kommt die Tatsache, dass dieses Kriterium bereits Hinweise auf einen ggf. eingeschränkten Anwendungsbereich gibt. Es wird unterschieden in implizite (bei Anwendung der Methode automatisch vorgenommene Prüfung der Risikoakzeptanz), explizite (Prüfung der Tolerierbarkeit eines ermittelten Risikos nach Abschluss der Methodenanwendung) und vergleichende Risikoakzeptanz (Risikoakzeptanz kann gezeigt werden, indem mit der gleichen Methode ermittelte Ergebnisse verglichen werden).

3.1.6 Aufbau und Diskussion der Klassifikation

Die endgültige Klassifikation ist Bild 3.1 zu entnehmen. Es ist eine dreistufige Klassifikation entstanden, wobei zwei Kriterien jeweils zwei unterschiedliche Optionen zulassen und das dritte Kriterium drei Wahlmöglichkeiten erlaubt. Die Klassifikation beinhaltet jedoch nicht alle möglichen Entscheidungsäste. Es wird davon ausgegangen, dass eine quantitative Methode immer auf einem mathematischen Modell beruhen muss. Die zukünftige Forschung wird dies zu validieren haben. Auch an anderen Stellen der Klassifikation besteht noch Forschungsbedarf. So muss beispielsweise diskutiert werden, ob intuitiv erstellte Methoden mit qualitativer

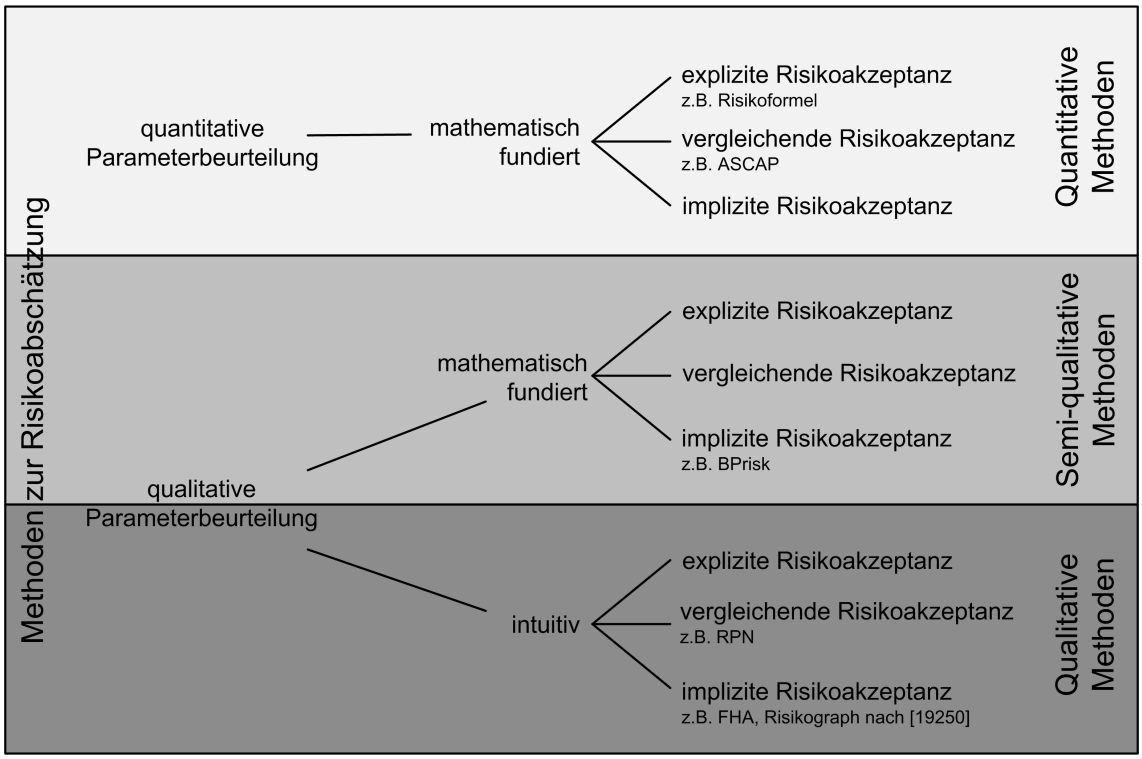

Bild 3.1: Klassifikation von Risikoabschätzungsmethoden

Parameterbeurteilung die explizite Prüfung der Tolerierbarkeit eines Ergebnisses überhaupt zulassen.

Methoden mit qualitativer Parameterbeurteilung werden im Weiteren als qualitative Methoden und Methoden mit quantitativer Parameterbeurteilung im Weiteren als quantitative Methoden bezeichnet. In der Literatur wird häufig der Begriff der semi-qualitativen bzw. semi-quantitativen Methoden verwendet. Beide Begriffe fortzuführen erscheint nicht zielführend, da dies aufgrund der phonetischen Ähnlichkeit zu Missverständnissen und Verwechslungen führen wird. Es wird vorgeschlagen, dass qualitative, modellbasierte Methoden als semi-qualitativ bezeichnet werden. Dies trägt der Tatsache Rechnung, dass diese Methoden trotz qualitativer Parameterbeurteilung auf einem quantitativen d.h. mathematisch fundierten Modell beruhen.

3.2 Der Risikograph

Mit dem Risikographen wird das von den Gefährdungen ausgehende Risiko ermittelt, d.h. es wird mit dem Risikographen eine Risikoabschätzung durchgeführt. Im Risikographen werden drei oder vier Parameter zur Beschreibung des Risikos miteinander verknüpft, wobei jeder Parameter in wenigen, im Allgemeinen zwischen zwei und vier Klassen, beschrieben wird. Üblicherweise enthalten Risikographen die Parameter

- Schadensausmaß,
- Aufenthaltsdauer im Gefahrenbereich bzw. Gefährdungsdauer/-häufigkeit,
- Gefahrenabwehr.

Häufig wird zusätzlich der Parameter Wahrscheinlichkeit des unerwünschten Ereignisses berücksichtigt. Die Parameter und im Besonderen die Parameterklassen sind überwiegend im Text beschrieben.

Das abgeschätzte Risiko wird im Allgemeinen nicht direkt ausgegeben. Es findet implizit innerhalb der Methode ein Vergleich zwischen abgeschätztem und tolerierbarem Risiko statt. Dem Anwender sind üblicherweise weder das abgeschätzte, noch das in der Methode hinterlegte, tolerierbare Risiko bekannt. Das Ergebnis der Risikographanalyse ist beispielsweise eine Risikoklasse, die ggf. mit einer Gefährdungsrate verknüpft ist.

Eine erste normative Veröffentlichung des Risikographen erfolgte in DIN V 19250 (1994)(zurückgezogen) *Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen (MSR: Meß-, Steuer-. Regelungseinrichtungen)*. Eine weitere, frühe Veröffentlichung eines Risikographen findet sich in der DIN EN 954 (1997). Die DIN EN 954 wurde 2006 ersetzt durch die Norm DIN EN ISO 13849-1 (2004), wobei der relevante Abschnitt zum Risikographen aus DIN EN 954 (1997) übernommen wurde.

Heute gibt es Risikographen in verschiedenen Normen für unterschiedliche Industriezweige. Diese sind teils zur Anwendung, teils als Beispiele vorgesehen:

- DIN EN ISO 13849-1 (Normentwurf): Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 1: Allgemeine Gestaltungsleitsätze
- DIN EN 61508-5: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/ programmierbarer elektronischer Systeme - Teil 5: Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität
- DIN EN 61511-3: Funktionale Sicherheit - Sicherheitstechnische Systeme für die Prozessindustrie - Teil 1: Allgemeines, Begriffe, Anforderungen an Systeme, Software und Hardware
- VDV-Schrift 332: Sicherheitsintegritätsanforderungen für Bahnsignalanlagen bei Nichtbundeseigenen Eisenbahnen (NE)

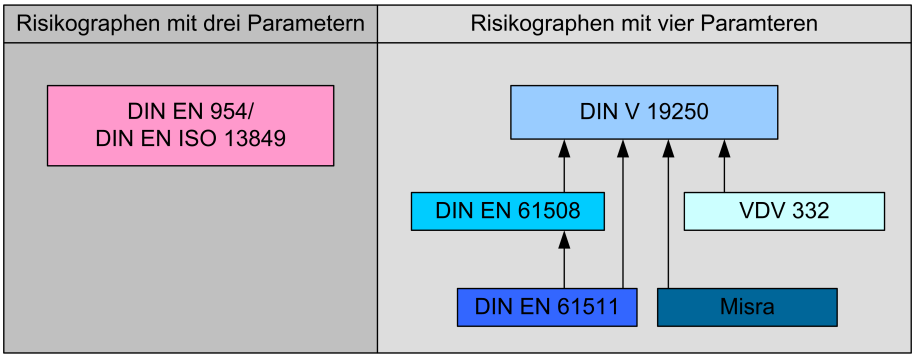

Bild 3.2: In den Normen angegebene, logische Abhängigkeiten zwischen den Risikographen

Wie eng die veröffentlichten Risikographen miteinander verzahnt sind, zeigt Bild 3.2. Die meisten Normen berufen sich auf den in DIN V 19250 veröffentlichten Risikographen als Grundlage. Es gibt Rückreferenzen. So unterscheidet DIN EN 61511 zwei Risikographen.

Kriterium	**DIN V 19250** (zurückgezogen)	**DIN EN ISO 13849**	**VDV 332 DIN EN 61508**
Anwendungs-ebene	MSR-Schutzfunktionen	Sicherheitsfunktion/ sicherheitsbezogene Teile von Steuerungen	Schutzfunktion/ sicherheitsbezogenes System
Parameterbetrachtung			
Anzahl	vier	drei	vier
Beschreibung/ Zahl d.Klassen	Schadensausmaß/Severity (4, 2)		Auswirkung (4)
	Aufenthaltsdauer im Gefahrenbereich (2)	Häufigkeit und/oder Dauer der Gefährdungsexposition (2)	Häufigkeit und Aufenthaltsdauer im gefährlichen Bereich (2)
	Gefahrenabwendung (2)	Möglichkeit zur Vermeidung der Gefährdung oder Begrenzung des Schadens (2)	Möglichkeit, den gefährlichen Vorfall zu vermeiden (2)
	Eintrittswahrscheinlichkeit des unerwünschten Ereignisses ohne Vorhandensein der MSR-Schutzeinrichtung (3)		Wahrscheinlichkeit des unerwünschten Ergebnisses (3)
Ergebnis	acht Anforderungsklassen	fünf Performance Level	acht Klassen a bis f

Tabelle 3.1: Vergleich der Methoden zur Risikoabschätzung (Werte in Klammern geben die Anzahl der Parameterklassen an)

Während zu einem Risikographen die DIN V 19250 als Grundlage genannt wird, wird beim zweiten Risikographen DIN EN 61508 als Basis genannt. In DIN EN 61508 wiederum wird ausdrücklich auf DIN V 19250 verwiesen.

Die Tabelle 3.1 stellt einige der Risikographen aus obiger Liste mit ihren wesentlichen Kenngrößen gegenüber. Die Risikographen aus DIN EN 61511-3 wurden nicht berücksichtigt, da diese im Wesentlichen aus anderen Normen direkt übernommen wurden. Die Tabelle zeigt, dass im grundsätzlichen Aufbau der Risikographen weitestgehend Übereinstimmung besteht.

Werden die im vorhergehenden Abschnitt identifizierten Kriterien für die Klassifikation von Verfahren zur Risikoabschätzung auf die genannten Risikographen angewendet, so ergibt sich die folgendende Einschätzung:

- Parameterbeurteilung: Der Anwender beurteilt die Gefährdung anhand von definierten Parameterklassen. Es steht keine kontinuierliche Skala zur Verfügung. Die Methoden sind daher als qualitativ zu bezeichnen.

- Modell der Methode: Zu den in den Normen und Richtlinien präsentierten Risikographen ist kein Risikomodell bekannt. Es ist aufgrund der Aussagen in den Dokumenten anzunehmen, dass es sich im Wesentlichen um die Anpassung bereits existierender Risikographen handelt. Es kann demnach nicht mathematisch gezeigt werden, ob die Parameterbeurteilungen zu rechnerisch richtigen Ergebnissen führen. Die Verfahren sind als intuitiv zu bezeichnen.

- Risikoakzeptanz: Ergebnis der Risikographen ist die Zuordnung der Gefährdung zu einer Risikoklasse. Das Ergebnis lässt Rückschlüsse darüber zu, welche Maßnahmen zu ergreifen bzw. welche Ausfallgrenzwerte einzuhalten sind. Solche Ergebnisse sind nur möglich, wenn das für die Gefährdung abgeschätzte Risiko mit einem tolerierbaren Ri-

siko verglichen wurde, bzw. eine Kalibrierung an einem festgesetzten Benchmarkwert erfolgte.

Die in den Normen und Richtlinien vorgegebenen Risikographen sind bei Anwendung der vorgestellten Klassifikation als qualitativ-intuitive Methoden zu bezeichnen. Während eine qualitative Parameterbeurteilung erwünscht ist, um den notwendigen Aufwand für Risikoabschätzungen zu minimieren, ist das fehlende Risikomodell negativ anzusehen, da im Zweifelsfall die Richtigkeit von Ergebnissen nicht geprüft werden kann. Um die Akzeptanz von qualitativen Methoden zu erhöhen, sollten zukünftig nur semi-qualitative Methoden verwendet werden, d.h. mathematisch fundierte, auf einem Risikomodell basierende Methoden.

3.3 Abgrenzung der Methode Risikograph

Viele qualitative und semi-qualitative Methoden zur Risikoabschätzung lassen sich in Form eines Risikographen darstellen. Der Unterschied eines Risikographen gegenüber beispielsweise einer als Risikograph dargestellten Risikomatrix oder einer als Risikograph dargestellten Risikoprioritätszahlenmethode besteht in der Berücksichtigung von Abhängigkeiten bei der Zuordnung der Anforderungsklassen. Wurde bei der Konstruktion eines Risikographen festgestellt, dass bestimmte Parameterkombinationen zum gleichen Ergebnis führen, dann kann dies im Risikographen festgehalten und der Risikograph dadurch verschlankt werden. Bild 3.3 verdeutlicht dies Prinzip: Im Risikographen werden vier verschiedene Parameter C, F, P und W unterschieden. Bei der Wahl der Paramterklasse C2 müssen Aussagen zu allen Parametern getroffen werden, um eine Anforderungsklasse zu erhalten. Wird jedoch zunächst die Parameterklasse C1 gewählt, kann direkt die Anforderungsklasse abgelesen werden. Wird die Parameterklasse C3 gewählt, kann auf den Paramter P verzichtet werden.

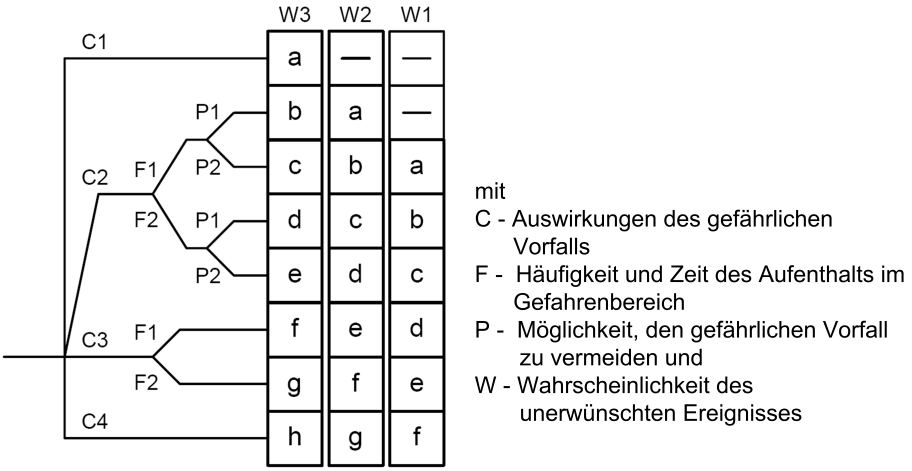

Bild 3.3: Der Risikograph aus VDV 332

Die Berücksichtigung von Abhängigkeiten im Risikographen bedeutet für den Anwender

- mehr Übersichtlichkeit, da die Auswirkungen der Parameterwahl offensichtlich sind,
- mehr Analyseverständnis, da die Bedeutung einzelner Parameter auf das Risiko offensichtlich werden,

- eine Beschleunigung der Analyse, da einige Parameter nicht beurteilt werden müssen.

Desweiteren lässt sich der Risikograph durch die Anzahl der zu berücksichtigenden Parameter bzw. Parameterklassen von anderen Methoden abgrenzen. Während die Risikomatrix sinnvollerweise nur für zwei Parameter aufgestellt werden kann (es gibt selten Varianten mit drei und vier Parametern), unterscheidet die Methode der Risikoprioritätszahlen drei Parameter mit je zehn Klassen. Während ein Risikograph mit nur zwei Parametern unterdimensioniert wäre, d.h. die Vorteile der Methode nicht zum Tragen kommen können, wäre ein Risikograph, der zehn Parameterklassen zulässt, unübersichtlich und nicht sinnvoll anwendbar. Ein Risikograph sollte zwischen 3 und 5 Parameter mit 2 bis 5 Parameterklassen berücksichtigen. Dies führt im Maximalfall zu 25 verschiedenen Ergebnisklassen. Damit ist eine Grenze dessen erreicht, was ergonomisch sinnvoll im Risikographen dargestellt werden kann.

Es können qualitative und semi-qualitative Risikographen unterschieden werden. Qualitative, intuitive Risikographen haben die in dem vorhergehenden Abschnitt beschriebenen Nachteile. Neue Risikographen sollten daher in jedem Fall modellbasiert sein, da nur die mit diesen Methoden erzielten Ergebnisse nachvollziehbar und überprüfbar sind. Die Begrenzung der Parameterzahl für einen Risikographen bedeutet nicht, dass die Zahl der im Modell zu berücksichtigenden Parameter begrenzt werden muss. Das der Methodenerstellung zu Grunde gelegte Risikomodell kann beliebig viele Parameter beinhalten; es sind jedoch Annahmen zu treffen, so dass im Endergebnis nur wenige variable Parameter im Risikographen verknüpft werden müssen.

3.4 Die Risikographen aus DIN EN ISO 13849-1 und aus VDV 332

Die Risikographen aus DIN EN ISO 13849-1 und aus VDV 332 sind typische Risikographen, d.h. sie gleichen in der Struktur einer Vielzahl weiterer Risikographen. Auf den ersten Blick scheinen die Methoden einfach und übersichtlich, sowie intuitiv anwendbar. Bei genauer Betrachtung offenbart sich jedoch, dass eine Vielzahl offener Fragen besteht. Die Analyse der Risikographen erfolgt anhand der in Abschnitt 2.5 gegebenen Gliederung. Die im Folgenden vorgestellte Zusammenstellung von Anwendungsproblemen und offenen Fragen ist nicht vollständig, zeigt jedoch deutlich, wo Verbesserungspotential besteht.

3.4.1 Der Risikograph in VDV 332

Vorstellung

Der Verband Deutscher Verkehrsunternehmen (VDV) stellt in seiner Schrift 332 *Sicherheitsintegritätsanforderungen für Bahnsignalanlagen bei Nichtbundeseigenen Eisenbahnen* den Anwendern einen Risikographen zur Ableitung von Sicherheitsanforderungen zur Verfügung. Der Risikograph ist in Bild 3.3 dargestellt.

Bei einer Risikoabschätzung mit dem VDV-Risikographen müssen bis zu vier Parameter für jeden bei einer Schutzfunktion auftretenden Fehler beurteilt werden (siehe Tabelle 3.2). Ergebnis der Analyse mit dem Risikographen ist eine notwendige minimale Risikominderung nach DIN EN 61508-1 bzw. eine Sicherheitsintegritätsstufe nach VDV.

Bezeichung	Bedeutung
Parameter: Auswirkungen des gefährlichen Vorfalls	
C1	geringe Verletzung
C2	schwere irreversible Verletzung einer oder mehrerer Personen oder Tod einer Person
C3	Tod mehrerer Personen
C4	Tod sehr vieler Personen
Parameter: Häufigkeit und Zeit des Aufenthalts im Gefahrenbereich	
F1	selten bis öfterer Aufenthalt im gefährlichen Bereich (vor allem für den technisch gesicherten Rückfallbetrieb sowie bei fahrer- und begleitlosen Systemen)
F2	häufiger bis dauernder Aufenthalt im gefährlichen Bereich
Parameter: Möglichkeit den gefährlichen Vorfall zu vermeiden	
P1	möglich unter bestimmten Bedingungen (anzusetzen bei Fahren auf Sicht)
P2	beinahe unmöglich (Standardannahme im normalen Betrieb)
Parameter: Wahrscheinlichkeit des unerwünschten Ereignisses	
W1	eine sehr geringe Wahrscheinlichkeit, dass die unerwünschten Ereignisse auftreten, und nur wenige unerwünschte Ereignisse sind wahrscheinlich, wenn das unerwünschte Ereignis zusätzlich vom Versagen einer weiteren, unabhängigen Schutzeinrichtung abhängt, jedoch dann nur mittelbar oder bedingt (z. B. beim Zusammentreffen zweier unabhängiger, betrieblicher Ereignisse) eintreten kann
W2	eine geringe Wahrscheinlichkeit, dass die unerwünschten Ereignisse auftreten, und wenige unerwünschte Ereignisse sind wahrscheinlich, wenn das unerwünschte Ereignis zusätzlich vom Versagen einer weiteren, unabhängigen Schutzeinrichtung abhängt, jedoch dann unmittelbar (z. B. durch menschliches Fehlverhalten) eintreten kann bzw. nur mittelbar oder bedingt (z. B. beim Zusammentreffen zweier unabhängiger, betrieblicher Ereignisse) eintreten kann
W3	eine relativ hohe Wahrscheinlichkeit, dass die unerwünschten Ereignisse auftreten, und häufige unerwünschte Ereignisse sind wahrscheinlich, wenn menschliches Fehlverhalten bei Nichtvorhandensein der Schutzeinrichtung möglich ist und das unerwünschte Ereignis dadurch unmittelbar eintritt

Tabelle 3.2: Beschreibung der Parameter des Risikographen aus VDV 332 (2008)

Arbeitsschritt Systemdefinition

Die Festlegung des Anwendungsbereichs einer Risikoabschätzungsmethode entspricht in den Aufgaben und Auswirkungen der Systemdefinition. Wird der Anwendungsbereich nicht eingehalten, können fehlerhafte Ergebnisse abgeleitet werden. Der Anwendungsbereich wird in VDV 332 (2008) wie folgt beschrieben *Die vorliegende Schrift gilt für Bahnsignalanlagen in regionalen Netzen Nichtbundeseigener Eisenbahnen (NE) des öffentlichen und nichtöffentlichen Verkehrs...Hierbei werden die heute bei NE-Bahnen bestehenden Verhältnisse mit Geschwindigkeiten bis zu 100 km/h zugrunde gelegt. Bei der durchzuführenden Betrachtung ist stets das Gefährdungspotenzial anzusehen, das ohne technische Sicherung des Prozesses entstehen würde. Für Bahnen mit Reisezugverkehr gilt im Sinne dieser Schrift, dass die Bahn der Abwicklung öffentlichen Reisezugverkehrs dient. Dies schließt die Abwicklung von Güterverkehr in beliebigem Umfang mit ein.*

Ein explizites Systemmodell wird nicht angegeben. Allerdings wird ausgeführt, dass *die aus dem Bahnbetrieb entstehenden Gefährdungen durch die vorgeschriebenen Maßnahmen abgedeckt sind.* Dies kann so interpretiert werden, dass eine Risikoabschätzung sich darauf beschränken darf, *jeder Schutzfunktion und den Anlagen und Einrichtungen, die diese Funktionen erfüllen, entsprechende Sicherheitsintegritätsanforderungen zuzuweisen.* Das System als solches ist demnach als Black Box zu betrachten. Für den Anwender erschwerend ist, dass es keine Begriffsdefinition gibt. Es ist beispielsweise nicht eindeutig, was unter einer Schutzfunktion zu verstehen bzw. was genau zu beurteilen ist. So wird zum einen ausgeführt, dass das Vorgehen auf die *Identifikation von Gefährdungen (im Sinne von Funktionsversagen)* abzielt, zum anderen jedoch, dass das Ergebnis Gefährdungen sind *(als Versagen der Schutzfunktion).* Nicht zuletzt heißt es *In dieser Schrift wird durch Grundsätze und Beispiele die Systematik aufgezeigt, mit der den in einer Risikoanalyse zu betrachtenden Einrichtungen die notwendigen minimalen Risikominderungen zugeordnet werden können.* Durch Betrachtung der Beispiele kann geschlussfolgert werden, dass Fehler der Schutzfunktion von Schutzeinrichtungen zu betrachten sind, wobei offen bleibt, wie genau eine Schutzeinrichtung definiert ist.

Arbeitsschritt Gefährdungsidentifikation

Detaillierte Informationen zur systematischen Gefährdungsidentifikation werden nicht gegeben. Es werden zu jeder Schutzfunktion *Auswirkungen von Fehlern* genannt.

Arbeitsschritt Risikoabschätzung und Zuweisung von Sicherheitsanforderungen

Das Ziel des Vorgehens wird in VDV 332 wie folgt beschrieben: Es wird *...ein Weg aufgezeigt, dass von einem abzuwickelnden technischen Prozess ausgehende Risiko für Bediener, Benutzer und die Umwelt darzustellen und die notwendigen Sicherheitsanforderungen in einer Klassifizierung zu ermitteln.*

Im Rahmen der Risikoabschätzung erfolgt keine detaillierte Diskussion der relevanten Unfallszenarien oder des Risikos. Im Besonderen wird kein Risikomodell entwickelt. Der Risikograph wird basierend auf den Risikographen in DIN V 19250 und DIN EN 61508-5 erstellt. Es erfolgt eine Kalibrierung, die jedoch keine Kalibrierung der Parameterklassenkombinationen mit den Ergebnisklassen ist, sondern eine Beschreibung von Parameterklassen.

Es wird ausgeführt, dass ggf. die zu schützenden Personen besonders zu definieren sind (z.B. Schutz des Zuges, Schutz des Individualverkehrs). Würde dem Risikographen ein kohärentes Risikomodell zu Grunde liegen, wäre eine solche Flexibilität nicht möglich. Es kann

immer nur das Risiko einer Betrachtungsgruppe abgeschätzt werden. Es wird nicht ausgeführt, welche Auswirkungen unterschiedliche Bezugsobjekte auf das Ergebnis haben. Insgesamt ist festzustellen, dass detaillierte Informationen zu dem der Methode zu Grunde liegenden System- und Risikomodell wünschenswert wären.

Die Beschreibung der Parameters *Auswirkung des gefährlichen Vorfalls C* geht ausschließlich von Personenschaden aus. Es werden keine Definitionen gegeben, was unter einer leichten bzw. schweren Verletzung zu verstehen ist. Wird die typischerweise zur Berechnung von Gesamtschaden bzw. Opfern verwendete Gleichung zu Grunde gelegt (siehe Abschnitt 4.9.4), haben alle Klassen eine unterschiedliche Bandbreite, d.h. die Schadensgrenzen haben keinen gleichbleibenden Abstand voneinander. Im Allgemeinen ist bei semi-qualitativen Risikoabschätzungsverfahren zwischen den Klassengrenzwerten ein gleichmäßer Abstand x bzw. entsprechend eine Potenz von x notwendig, um im Ergebnis eine gleichmäßige Verteilung der Ergebnisklassen zu erhalten. Grundsätzlich ist es vorstellbar, dass von einer gleichmäßigen Verteilung der Parameterklassengrenzen Abstand genommen wird, um beispielsweise den Effekt der Risikoaversion zu berücksichtigen. Ob dies bei dem vorliegenden Risikographen der Fall ist, kann nicht entschieden werden, da weder in VDV 332 (2008) noch in der Literatur Aussagen dazu getroffen werden. Die Klasse C1 wird als geringe Verletzung beschrieben. Da hier die Einzahl gewählt wurde, wird nur eine Person betrachtet. Eine solche detaillierte Betrachtung ist jedoch in einem qualitativen Verfahren im Allgemeinen nicht sinnvoll und nur geeignet, wenn im Risikomodell festgelegt ist, dass von einem Versagen nur eine Person betroffen ist. C1 soll auch gewählt werden, wenn eine Verletzung von Personen ausgeschlossen ist. In diesem Fall besteht jedoch kein relevantes Risiko (wenn angenommen wird, dass der Risikograph Risiko aus Personenschaden abschätzt). Daher sollte eine Trennung der Kategorien bzw. die Einführung einer zusätzlichen Kategorie für nicht analyserelevanten Schaden vorgenommen werden. Die Kategorie C2 gilt für schwere, irreversible Verletzungen. Es fehlt zwischen den Kategorien C1 und C2 eine Katgeorie für mittlere Verletzungen, z.B. schwere, reversible Verletzungen. Es ist nicht klar, wo eine Eingruppierung für Ereignisse erfolgt, die z.B. zu vielen leichten Verletzungen führen. In den Erläuterungen wird ausgeführt, dass im Allgemeinen beim Reisezugbetrieb Schadensklasse C3, d.h. mehrere Tote, zu wählen ist. Die Erfahrung zeigt jedoch, dass es nur in seltenen Fällen tatsächlich zu mehreren Toten kommt. Es ist zu vermuten, dass durch eine stärkere Berücksichtigung der betrieblichen Charakteristika häufig der Parameter C2 das Schadensausmaß adäquat beschreibt. Es wird eine Schadensklasse C4 definiert, die aber laut Erläuterungstext nicht relevant ist. Ist dies der Fall, ist zu diskutieren, ob sie überhaupt aufgeführt werden sollte.

Die Beschreibung des Parameters *Aufenthalt im Gefahrenbereich F* lässt Disskussionsspielraum, da die Grenzen zwischen öfter und häufig nicht definiert sind. Es wäre hier besser, wenn die Informationen aus dem erläuternden Text direkt in die Parameterbeschreibung einfließen würden.

Der Parameter *Möglichkeit den gefährlichen Vorfall zu vermeiden P* fällt dadurch auf, dass er wenig Spielraum für eine detaillierte Abschätzung bzw. Beschreibung der tatsächlich vorhandenen Abwehrmechanismen lässt. Die zugehörige Erläuterung weist an, dass in fast allen Fällen P2, d.h. beinahe unmöglich, zu wählen ist. Es erscheint, dass dieser Wert zwar auf der sicheren Seite ist, aber dazu beitragen wird, dass tendenziell zu konservative Anforderungen abgeleitet werden. Werden die betrieblichen Charakteristika auf Strecken von Nichtbundeseigenen Eisenbahnen in Betracht gezogen, im Besonderen die tendenziell geringen Geschwindigkeiten, erscheint eine Klassifikation der Vorfallvermeidung als beinahe unmöglich nicht sinnvoll.

Bei einer Betrachtung der Angaben zum Parameter W fallen vor allem die wenig verständlichen Erläuterungen auf, vor allem oder gerade weil es zwei getrennte Parameterklassenbeschreibungen gibt. Die Angabe von zwei unterschiedlichen Klassifikationen für W führt zu Diskussionen, wenn dies zu einer unterschiedlichen Eingruppierung des betrachteten Fehlers führt. Es ist nicht nachzuvollziehen, was genau mit dem Parameter abzuschätzen ist. Ein Beispiel für eine solche missverständliche Aussage ist: *Grad des menschlichen Fehlverhaltens ohne zu benutzende Schutzeinrichtung.* In den Beispielen sind z.B. Endlagenüberwachung und Weichenverschluss Schutzeinrichtungen. Diese können nicht durch Menschen ersetzt werden.

In Bild 3 der VDV 332 wird auf eine Zuordnung der notwendigen Risikominderung zu Sicherheitsintegritätsstufen verwiesen. Diese Zuordnung wurde aus DIN EN 61508-5 übernommen. Dort ist sie jedoch nur als Beispiel gegeben. Eine Übernahme ohne Begründung und Herleitung ist abzulehnen. Dies ist besonders wichtig, da es bei der Zuordnung zu Sprüngen der Klassen kommt, d.h. keine gleichmäßige Verteilung der Ergebnisklassen erfolgt. Dies sollte begründet werden.

Es werden Bedingungen genannt, unter denen eine Reduzierung der Sicherheitsanforderungen erfolgen kann. Es wird dafür keine Begründung gegeben. Die Erläuterungen sind missverständlich.

Fazit

Zusammenfassend kann festgestellt werden, dass die Beschreibung des Risikographen in der VDV-Richtlinie nicht ausreichend ist, dem Anwender nachvollziehbar die Grundlagen des Risikographen und dessen Anwendung zu vermitteln. Um zu überprüfen, ob der Risikograph mit den ihm hinterlegten Annahmen dazu geeignet ist, im Rahmen eines spezifischen Projekts angewendet zu werden (d.h. um zu prüfen, ob die ermittelten Anforderungsklassen übernommen werden können, wie es die Schrift VDV 334 fordert), ist das Dokument nicht geeignet.

Anhand des Beitrags von Peters u. a. (2005) kann für das Beispiel Fahrzeuggerät der Zugbeeinflussung gezeigt werden, dass der VDV-Risikograph anscheinend nicht nur ungünstig beschrieben und unvollständig ist, sondern auch die ermittelten Ergebnisse konservativ sind. In VDV 332 (2008) wird abgeleitet, dass die von einer punktförmigen Zugbeeinflussungseinrichtung nachzuweisende Sicherheitsintegritätsstufe drei ist. In dem Beitrag von Peters u. a. (2005) wird beschrieben, wie quantitative Sicherheitsziele für eine punktförmige Zugbeeinflussung durch Betrachtung der Ausfallraten des Fahrzeuggeräts ermittelt wurden. Es wird ausgeführt, dass es sich um ein einkanaliges Rechnersystem mit Selbsttestfunktion („Watchdog“) handelt. In DIN EN 50129 (2003), Tabelle E.4 wird gegenübergestellt, welche Sicherheitsintegritätsstufe mit welcher technischen Realisierung möglich ist. Das in Peters u. a. (2005) beschriebene System entspricht einer einkanaligen, elektronischen Struktur mit Selbsttest und Überwachung, womit ein SIL 1 oder SIL 2 erreicht werden kann. Den in Peters u. a. (2005) dargestellten Fehlerbäumen kann entnommen werden, dass die realisierte Funktion vermutlich einem SIL 1 einspricht, in jedem Fall nicht dem in VDV 332 (2008) für Nichtbundeseigene Eisenbahnen abgeleiteten SIL 3. Auch wenn zu hohe Anforderungen zu sicheren Systemen führen, so bedeutet dies auch, dass die Systeme teurer und damit unwirtschaftlicher werden.

3.4.2 Der Risikograph in DIN EN ISO 13849-1

Vorstellung

DIN EN ISO 13849-1 gibt einen Risikographen vor, der dazu dient *einen PL_r für jede notwendige, durch ein SRP/CS auszuführende Sicherheitsfunktion auszuwählen.* Die folgenden

Definitionen aus der Norm sind für das Verständnis der Aussage von Bedeutung:

- PL (Performance Level): diskreter Level, der die Fähigkeit von sicherheitsbezogenen Teilen einer Steuerung spezifiziert, eine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen
- PL_r (erforderlicher Performance Level): angewandter Performance Level, um die erforderliche Risikominderung für jede Sicherheitsfunktion zu erreichen.
- SRP/CS (Sicherheitsbezogenes Teil einer Steuerung): Teil einer Steuerung, das auf sicherheitsbezogene Eingangssignale reagiert und sicherheitsbezogene Ausgangssignale erzeugt
- Sicherheitsfunktion: Funktion einer Maschine, wobei ein Ausfall der Funktion zur unmittelbaren Erhöhung des Risikos (der Risiken) führen kann

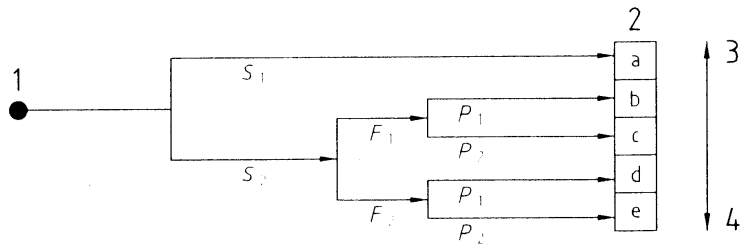

Bild 3.4: Der Risikograph aus DIN EN ISO 13849-1

Der in der Norm beschriebene Risikograph ist Bild 3.4 zu entnehmen. Die zur Beurteilung heranzuziehenden Parameter sind in Tabelle 3.3 dargestellt. Es wird in der Norm davon ausgegangen, dass die Anforderung der Sicherheitsfunktion häufiger als einmal pro Jahr erfolgt.

Arbeitsschritt Systemdefinition

Es werden keine Aussagen zum Systemmodell getroffen.

Ausgangssituation für die Risikobetrachtung ist die Situation vor Bereitstellung der Sicherheitsfunktion. Andere Maßnahmen zur Risikoreduktion können in der Analyse berücksichtigt werden: *Die Risikominderung durch andere technische Maßnahmen, die unabhängig von der Steuerung sind (z.B. mechanische trennende Schutzeinrichtungen) oder zusätzliche Sicherheitsfunktionen, können bei der Bestimmung des PL_r der vorgesehenen Sicherheitsfunktion berücksichtigt werden.*

Arbeitsschritt Gefährdungsidentifikation

Der Begriff der Gefährdung (*potentielle Schadensquelle*) ist unzureichend und der Begriff der Gefährdungsexposition ist in der Norm nicht definiert.

Bez.	Bedeutung	Erläuterung
Schaden S		
S1	leichte Verletzungen (üblicherweise reversibel)	Quetschungen und/oder Fleischwunden ohne Komplikationen
S2	ernste Verletzungen (üblicherweise irreversibel und Tod)	Amputation oder Tod
Häufigkeit und/oder Dauer der Gefährdungsexposition F		
F1	selten bis weniger häufig und/oder die Zeit der Gefährdungsexposition ist kurz	
F2	häufig bis dauernd und/oder die Zeit der Gefährdungsexposition ist lang	es ist unerheblich, ob dieselbe oder nacheinander unterschiedliche Personen der Gefährdung ausgesetzt sind, z.B. bei Aufzügen
Möglichkeit der Vermeidung der Gefährdung oder Begrenzung des Schadens P		
P1	möglich unter bestimmten Bedingungen	wenn realistische Chance besteht, den Unfall zu vermeiden oder dessen Auswirkungen maßgeblich zu reduzieren
P2	kaum möglich	

Tabelle 3.3: Beschreibung der Parameter des Risikographen aus DIN EN ISO 13849-1

Arbeitsschritt Risikoabschätzung

Die Ausführungen machen deutlich, dass es die Aufgabe des Risikographen ist, die mit der betrachteten Sicherheitsfunktion zu erreichende, notwendige Risikominderung zu ermitteln. Dazu muss mit dem Risikographen das Risiko des Ausgangssystems ohne Sicherheitsfunktion(en) abgeschätzt werden. Die Sicherheitsfunktion dient ausschließlich der Risikominderung. In der Norm wird kein Risikomodell abgebildet, anhand dessen die relevanten Informationen beispielsweise bezüglich Risikoart abgelesen werden können. Das ermittelte Ergebnis kann deshalb nicht auf seine Richtigkeit überprüft werden. Die Wirkungsweise der einzelnen Parameter kann nicht nachvollzogen werden.

Die Norm DIN EN ISO 13849-1 gibt Hinweise zur Wahl des Parameters Schadensausmaß. So heißt es dort, dass Verletzungen zu betrachten sind, die *...durch Ausfall einer Sicherheitsfunktion...* entstehen. Dazu muss jedoch nicht das von der Funktion ausgehende Risiko abgeschätzt werden, sondern das von der Sicherheitsfunktion ausgehende Risiko. Hinzu kommt, dass laut Aussagen der Norm die Situation ohne Sicherheitsfunktion zu analysieren ist. Richtiger müsste es heißen, dass das Schadensausmaß bei Ausfall der Funktion zu analysieren ist. Zusätzlich (und in einem späteren Schritt) muss sichergestellt werden, dass das zusätzliche, von der Sicherheitsfunktion ausgehende Risiko nicht unzulässig groß wird.

Bei den bisher in Deutschland durchgeführten Sicherheitsbetrachtungen wurde Personenschaden in leicht und schwer verletzte sowie getötete Personen unterschieden. Eine Eingruppierung dieser drei Kategorien in die Klassen des Risikographen ist nicht offensichtlich. Leichte Verletzungen sind im Allgemeinen als reversibel zu klassifizieren. Ebenfalls einfach ist die Eingruppierung von tödlichen Verletzungen; diese sind stets irreversibel. Die Eingruppierung von schweren Verletzungen (z.B. komplizierten Beinbrüchen) ist schwierig und mit den gegebenen Definitionen nicht eindeutig möglich, da schwere Verletzungen sowohl reversibel als auch

irreversibel sein können.

Der Parameter Schadensausmaß berücksichtigt, so wie er in der Norm beschrieben wird, nur Personenschaden; es wird entweder ein kollektives oder individuelles Personenrisiko ermittelt. Die Norm geht nicht darauf ein, ob der gesamte Personenschaden aller potentiell betroffenen Personengruppen oder nur ausgewählter Personenschaden zu betrachten ist. Es wird nicht darauf eingegangen, ob und wie Schaden an mehreren Personen (z.B. viele geschädigte Personen mit jeweils leichten Verletzungen im Unterschied zu einer schwerverletzten Person) zu berücksichtigen ist.

Die Verknüpfung der beiden Aspekte Dauer und Häufigkeit der Gefährdungsexposition zu einem Parameter ist schwierig und nicht eindeutig. In Tabelle 3.4 sind die verschiedenen möglichen Kombinationen eingeordnet.

		Häufigkeit		
		Keine Angaben	Kurze Gefährdungs-exposition	Lange Gefährdungs-exposition
Dauer	Keine Angaben		F1	F2
	Selten bis weniger häufig	F1	F1	F1 oder F2
	Häufig bis dauernd	F2	F1 oder F2	F2

Tabelle 3.4: Interpretation des Parameters F des Risikograophen aus DIN EN ISO 13849-1

Es werden Beispiele für die bei der Beurteilung des Parameters Gefährdungsvermeidung P zu berücksichtigenden Einflüsse gegeben. Es wird deutlich, dass sowohl technische als auch menschliche Einflüsse zu berücksichtigen sind. Einige der gegebenen Beispiele sind externe Faktoren (z.B. Eingreifen Dritter), andere Faktoren sind durch das System bestimmt (z.B. Geschwindigkeit, mit der sich die Gefährdung entwickelt). Es ist zu diskutieren, ob es sinnvoll ist, davon auszugehen, dass dieser Parameter, wie implizit im Namen vorgegeben, die Gefährdungsvermeidung beschreibt. Prinzipiell kann an zwei Punkten im Ablauf vom funktionierenden System zum Unfall eingegriffen werden: Maßnahmen können auf eine Gefährdungsvermeidung oder eine Unfallvermeidung abzielen. Die gegebene Beschreibung des Parameters ist nicht eindeutig. Beide Ansätze sind grundsätzlich sinnvoll und haben ihre Berechtigung: So kann beispielsweise das Senken der Ausfallrate der Betrachtungseinheit dazu führen, dass es weniger Gefährdungen gibt. Andererseits kann bei gleichbleibender Gefährdungsrate durch sinnvolle Maßnahmen, wie beispielsweise zügige Offenbarung der Gefährdung, dazu beigetragen werden, dass nach Auftreten der Gefährdung die Zahl der Unfälle reduziert werden kann. Zum Teil sind auch die zu berücksichtigenden Einflüsse sehr ähnlich: So spielt die Geschwindigkeit, mit der sich eine Gefährdung entwickelt unter Umständen die gleiche Rolle wie die Geschwindigkeit, mit der sich ein Unfall entwickelt. Es ist davon auszugehen, dass sowohl Maßnahmen zur Gefährdungsvermeidung wie zur Unfallvermeidung kombiniert werden. Der Parameter kann jedoch nicht beide Einflüsse erfassen, sondern es muss eine eindeutige Regelung gefunden werden. Wenn der Parameter die Möglichkeit zur Gefährdungsvermeidung beschreiben würde, würde er in direktem Zusammenhang zum Parameter Gefährdungsexposition stehen. Erst wenn der Parameter Gefährdungsvermeidung klar definiert wurde, kann darauf basierend der Parameter Gefährdungsexposition ermittelt werden. Für die Ermittlung des Risikos, im Besonderen der Unfallhäufigkeit, ist es jedoch ausreichend, wenn die tatsächlich vorhandene Zahl an Gefährdungen bekannt ist, auf der aufbauend die Unfallzahl abgeschätzt werden kann. Deshalb erscheint es sinnvoll, den Parameter als Möglichkeit zur Unfallver-

meidung zu beschreiben. Der Parameter, bezeichnet mit dem Formelzeichen P, umfasst alle Einflüsse, die dazu beitragen, dass sich aus einer Gefährdung kein Unfall entwickelt.

Es gibt keinen Parameter für die Wahrscheinlichkeit eines unerwünschten Ereignisses. Dadurch kann beispielsweise nicht berücksichtigt werden, wenn es nur dann zum Unfall kommt, wenn weitere, unabhängige betriebliche Ereignisse hinzukommen, bzw. weitere Schutzfunktionen versagen.

Fazit

Bei einer detaillierten Betrachtung des Risikographen und seiner Beschreibung wurde eine Vielzahl von Fragen aufgeworfen, die vor einer weiteren Anwendung des Risikographen zu diskutieren sind.

3.5 Anforderungen an Risikographen

Der im Rahmen der Arbeit zu erstellende Risikograph wird wie folgt definiert:

Der Risikograph ist eine semi-qualitative Methode zur Risikoabschätzung. Der Risikograph basiert auf einem aus mehreren Parametern zusammengesetzten Risikomodell, wobei im Graphen im Allgemeinen drei bis fünf Parameter des Risikomodells abgebildet sind. Für weitere Parameter sind ggf. Annahmen zu treffen und zu dokumentieren. Die Parameter werden im Risikographen verknüpft, wobei Abhängigkeiten dazu führen können, dass nicht alle möglichen Entscheidungspunkte im Graphen berücksichtigt werden müssen.

Im Abschnitt 3.4 wurde eine Reihe von Aspekten herausgearbeitet, die bei der Anwendung der beispielhaft analysierten Risikographen zu Schwierigkeiten führen können. Die gemachten Erfahrungen lassen sich auf andere Risikographen übertragen. Es lassen sich die folgenden Anforderungen an Risikographen ableiten:

- eindeutige Definition aller maßgeblichen Begriffe,
- klare und nachvollziehbare Beschreibung der Risikographanwendung,
- kohärente, nachvollziehbare und einfach anwendbare Beschreibung der Parameterklassen,
- Definition eines System- und Risikomodells, um den Zusammenhang der Parameter und die der Konstruktion zu Grunde gelegten Annahmen und Bedingungen nachvollziehen zu können,
- nachvollziehbare Zuordnung der Parameterklassenkombinationen zu den Ergebnissen.

In Braband (2005) wird zu Risikographen ausgesagt, dass nachteilig ist, dass

- es keine Angaben zur Konstruktion der bereits eingesetzten Risikographen gibt und damit die Ergebnisse nicht überpüft werden können,
- die Risikoaktzeptanz zwar im Risikographen im Allgemeinen enthalten ist, nicht jedoch überprüft werden kann,
- durch ausschließlich verbale Beschreibung der Parameterklassen ein relativ großer Ermessensspielraum für den Anwender besteht,

- die Gefährdungsdauer nicht berücksichtigt wird und es keine Angaben zur Gefährdungsoffenbarung gibt.

Den ersten beiden Kritikpunkten kann durch die Konstruktion eines Risikographen basierend auf einem Risikomodell entgegengewirkt werden. Inwieweit die Gefährdungsdauer zu berücksichtigen ist bzw. Aussagen zur Gefährdungsoffenbarung zu treffen sind, muss im Rahmen der Modellerstellung diskutiert werden. Hinsichtlich der Beschreibung der Parameterklassen sollte versucht werden, wahlweise durch detailliertere Beschreibungen den Ermessensspielraum gering zu halten oder neue Möglichkeiten der Parameterklassenbeschreibung zu finden.

Braband stellt in Braband (2005) sieben Anforderungen an Risikobewertungsmethoden zusammen:

1. Als Risikoakzeptanzkriterium sollte Mindestens gleiche Sicherheit (MGS) zugrunde gelegt werden.
2. Es ist nicht notwendig, das Restrisiko explizit auszuweisen.
3. Das zugrunde liegende Modell soll Mensch und Technik umfassen.
4. Jede Systemfunktion sollte unabhängig von allen anderen bewertet werden können.
5. Die Schadensanalyse sowie die Folgenanalyse sollte qualitativ nach vorgegebenen, einheitlichen Kategorien oder mit standardisierten Reduktionsfaktoren erfolgen.
6. Es sollten alle relevanten Parameter berücksichtigt werden.
7. Die Aussagegenauigkeit des Verfahrens sollte innerhalb einer Zehnerpotenz liegen.

Die unter Punkt eins genannte Anforderung ist auch unter Berücksichtigung von Verordnung EG Nr. 352/ (2009) zulässig. In Verordnung EG Nr. 352/ (2009) heißt es : *Weist der Vorschlagende jedoch nach, dass das nationale Sicherheitsniveau im betreffenden Mitgliedstaat sich auch bei einer Ausfallrate pro Betriebsstunde von über* 10^{-9} *aufrechterhalten lässt, kann das entsprechende Kriterium vom Vorschlagenden im betreffenden Mitgliedstaat angewandt werden.* Wenn der mit MGS abgeleitete Wert der Forderung der Verordnung entspricht, kann MGS angewendet werden

Eine Ausweisung des Restrisikos, d.h. des tatsächlich bestehenden bzw. des der Konstruktion zu Grunde gelegten Risikos, erfolgt bei einer Risikoabschätzung mit Risikographen nicht.

Inwieweit ein Risikograph immer Mensch und Technik umfassen muss, ist fraglich. Es ist wünschenswert und entspricht der Praxis in z.B. VDV 332 (2008) den Risikographen ausschließlich zur Beurteilung von Technik vorzusehen. Dies ist auch unter dem Gesichtspunkt der Anwendung von RAC-TS als Risikoakzeptanzkriterium sinnvoll.

Die Unabhängigkeit der Systemfunktionen muss im Rahmen der Systemdefinition sichergestellt werden. Trotz der Unabhängigkeit der Systemfunktionen ist davon auszugehen, dass Anforderungen an das Zusammenspiel von Funktionen zu stellen sind. Dies sollte bei der Erstellung des Risikomodells berücksichtigt werden. Gleiches gilt für die Berücksichtigung aller Parameter der Risikoformel im Risikomodell (Punkt sechs).

Punkt fünf beschreibt das grundlegende Wesen der Risikoabschätzung mit dem Risikographen.

Eine Aussage zur Genauigkeit einer qualitativen Risikoabschätzungsmethode ist schwierig zu treffen. Für den Risikographen ist eine Genauigkeitsbetrachtung erst möglich, wenn Erfahrungen mit der Anwendung eines semi-qualitativen Risikokgraphen vorliegen.

Kapitel 4

Einflüsse auf die Risikographkonstruktion

4.1 Vorgehen

Im folgenden Kapitel werden die wesentlichen Aspekte, die bei der Konstruktion von Risikographen für die Anwendung im Eisenbahnwesen zu berücksichtigen sind, diskutiert. Im Wesentlichen gelten die gemachten Aussagen für alle qualitativen und semi-qualitativen Risikoabschätzungsmethoden. Lediglich wenn es um die Wahl der in der Methode zu berücksichtigenden Parameter zur Risikobeschreibung und deren Interpretation geht, ergibt sich durch die Beschränkung der Parameteranzahl im Risikographen eine Beschränkung auf diese Methode. Der Einfachheit halber wird daher im Folgenden stets von Aspekten für die Konstruktion eines Risikographen gesprochen. Die Übertragung der Informationen auf andere Methoden bleibt dem Leser überlassen.

Die Schritte des Lebenszyklusprozesses können als Anhaltspunkte für den Konstruktionsprozess von Risikographen dienen. Der Konstrukteur des Risikographen hat die Aussagen der Norm übergreifend und generisch zu interpretieren, so dass eine Anwendung der Methode für den geplanten Anwendungsbereich erfolgen kann. Im Folgenden wird der Ablauf der Risikographkonstruktion anhand der Beschreibung der relevanten Phasen des Lebenszyklusprozesses Systemdefinition, Risikoanalyse und Systemanforderungen in der DIN EN 50126 (2000) abgeleitet. Dabei wird davon ausgegangen, dass der Begriff *Gefahren* (wie in DIN EN 50126 (2000) verwendet) gleichzusetzen ist mit dem Begriff *Gefährdungen*.

In DIN EN 50126 (2000) heißt es zur Phase Systemdefinition : *Diese Phase hat folgende Zielsetzungen:*

1. *Festlegung des Betriebsaufgaben-Profils des Systems;*
2. *Festlegung der Systemgrenzen;*
3. *Erstellen der Anwendungsbedingungen, die die Systemmerkmale beeinflussen;*
4. *Festlegung des Umfangs der Systemgefahrenanalyse (Hazard Analysis);*
5. *...*

soweit sie die mögliche RAMS-Performance des Systems betreffen.

Der Punkt Festlegung des Betriebsaufgaben-Profils des Systems kann interpretiert werden als Festlegung, was der Risikograph erreichen soll. Dies umfasst die Art und Aussagekraft des Ergebnisses. Eine Festlegung der Systemgrenzen ist nur möglich, wenn ein der Konstruktion zu Grunde zu legendes Systemmodell erstellt wurde. Art und Umfang sowie Beschreibung des Systemmodells sind vom Anwendungsbereich des Risikographen abhängig. Das Zusammentragen der Anwendungsbedingungen ist gleichzusetzen mit einer Beschreibung der Systemumgebung. Die Festlegung des Umfangs der Systemgefahrenanalyse findet seine Entsprechung in der Beschreibung der Analyseebene.

In DIN EN 50126 (2000) heißt es zur Phase Risikoanalyse: *Diese Phase hat folgende Zielsetzungen:*

1. *Identifikation von Gefahren, die mit dem System verbunden sind;*
2. *Identifikation der Ereignisse, die diese Gefahren auslösen;*
3. *Bestimmung des mit den Gefahren verbundenen Risikos;*
4. *...*

Die Identifikation der Gefährdungen für ein System beruht im Allgemeinen auf der Betrachtung der Ausfälle bzw. Versagen der Funktionen des Systems. Daher sind grundlegende Überlegungen zur Funktion als Teil der Gefährdungsidentifikation zu sehen. Die eigentliche Gefährdungsidentifikation ist abhängig von der Definition des Begriffs der Gefährdung und der Festlegung aller wesentlichen, eine Gefährdung beschreibenden Bedingungen. Sekundär die Gefährdungen, aber primär die Funktionen sind in ihrer Beschreibung und ihrem Detaillierungsgrad abhängig von der gewählten Analyseebene.

Es muss im Rahmen der Risikographkonstruktion keine Betrachtung der Ursachen für die Gefährdungen erfolgen.

Die Ermittlung der mit den Gefährdungen verbundenen Risiken erfordert eine detaillierte Auseinandersetzung mit dem Risikobegriff, den das Risiko definierenden Parametern und ihren Einflussgrößen. Es sind Überlegungen zum maßgeblichen Szenario der Risikobetrachtung notwendig. Es ist ein Risikomodell zu erstellen. Es sind die Parameter auszuwählen, die im Risikographen beurteilt werden sollen. Es sind Parameterklassen festzulegen.

In DIN EN 50126 (2000) heißt es zur Phase Systemanforderungen: *Diese Phase hat folgende Zielsetzungen:*

1. *Spezifikation der gesamten RAMS-Anforderungen für das jeweilige System;*
2. ...

Übertragen auf die Risikographkonstruktion kann die Aufgabe dieser Phase beschrieben werden als Ableitung der Sicherheitsanforderungen. Dies hat basierend auf dem abgeschätzte Risiko zu erfolgen. Damit dies mittels Risikograph möglich ist, muss ein Risikoakzeptanzkriterium festgelegt werden und eine Kalibrierung des Risikographen erfolgen.

Daraus ergeben sich die folgenden Arbeitsschritte für die Konstruktion eines Risikographen:

- Festlegen des Anwendungsbereichs,
- Festlegen der Ergebnisart,

- Erstellung eines Systemmodells,
- Festlegen der Analyseebene,
- Definition von Funktion und Gefährdung,
- Gefährdungsidentifikation,
- Definition und Diskussion des Risikomodells,
- Generische Beschreibung des maßgeblichen Szenarios zur Risikoabschätzung,
- Wahl der Parameter des Risikographen,
- Wahl der Parameterklassen,
- Kalibrierung des Risikographen.

4.2 Anwendungsbereich eines Risikographen

Die Konstruktion eines Risikographen basiert auf Annahmen und Randbedingungen zu den zu analysierenden Funktionen. Nur wenn bei der Anwendung eines Risikographen diesen Annahmen und Randbedingungen entsprochen wird, können angemessene und im Rahmen der Genauigkeit richtige Ergebnisse ermittelt werden. Annahmen und Randbedingungen sind in Abhängigkeit des gewünschten Anwendungsbereichs zu wählen.

Der Anwendungsbereich eines Risikographen kann in Abhängigkeit von der Art des Sicherheitsnachweises definiert werden. In DIN EN 50129 (2003) wird ausgeführt, dass drei Kategorien von Sicherheitsnachweisen zu unterscheiden sind:

- *generischer Produktsicherheitsnachweis (unabhängig von der Anwendung)*
- *generischer Anwendungssicherheitsnachweis (für eine Klasse von Anwendungen)*
- *spezifischer Anwendungssicherheitsnachweis (für eine spezifische Anwendung)*

In Anlehnung daran können Risikographen hinsichtlich ihres Anwendungsbereiches unterschieden werden in

- generische Risikographen,
- generisch-anwendungsbezogene Risikographen und
- spezifische Risikographen.

Mit generischen Risikographen können, ggf. unter Berücksichtigung von Randbedingungen, unterschiedliche, unabhängige Anwendungen analysiert werden. Ein typischer generischer Risikograph ist der Risikograph in DIN EN ISO 13849-1 (2004), welcher für aus Maschinenversagen resultierende Gefährdungen angewendet werden kann. Der Vorteil generischer Risikographen ist, dass nur einmal mit ggf. großem Aufwand ein Risikograph zu erstellen und zu kalibrieren ist, der in der Folge vielfältig eingesetzt werden kann. Schwierig ist dabei, dass der Anwender sicherstellen muss, dass die bei der Risikographerstellung zu Grunde gelegten Annahmen für

den vorgesehenen Einsatzbereich allgemeingültig sind. Die Beschreibung und die Wahl der Risikographparameter muss aufgrund des großen Anwendungsbereichs allgemein gehalten sein. Dies kann zur Folge haben, dass die Ergebnisse der Risikoabschätzung zwar auf der sicheren Seite liegen, jedoch bei der Anwendung zu unwirtschaftlichen Lösunegn führen.

Generisch-anwendungsbezogene Risikographen sind auf eine beschränkte Gruppe von Anwendungen anwendbar. Ein Beispiel dafür ist der Risikograph in VDV 332, welcher nur für Bahnsignalanlagen von Nichtbundeseigenen Eisenbahnen gültig ist. Aufgrund des beschränkten Anwendungsbereichs ist es einfacher, die der Risikographerstellung zu Grunde gelegten Annahmen zu rechtfertigen. Es ist möglich, das Risiko detaillierter abzubilden und so exakter abzuschätzen.

Spezifische Risikographen sind nur für eine spezielle Anwendung, beispielsweise ein Produkt anwendbar. Der Erstellungsprozess ist vereinfacht, weil die Randbedingungen genau bekannt sind. Das Risiko kann exakter beschrieben werden als durch generische Risikographen. Es ist jedoch zweifelhaft, ob der Aufwand für das Erstellen und Kalibrieren eines solchen Risikographen gerechtfertigt ist. Daher ist ein solches Vorgehen abzulehnen.

4.3 Ergebnisart

Unter Berücksichtigung der Aussagen in den Normen sind unterschiedliche Ergebnisarten bei der Anwendung eines Risikographen möglich.

In DIN EN 61508-1 (2002) wird zunächst das relevante Risiko abgeschätzt und darauf basierend Gesamtsicherheitsanforderungen in Form von Angaben zur notwendigen Risikoreduktion durch die Sicherheitsfunktionen abgeleitet. Die Ableitung der notwendigen Risikoreduktion ist notwendig, um die Anforderungen zur Sicherheitsintegrität (Sicherheitsintegritätslevel/Safety Integrity Level SIL) zu bestimmen. Dies entspricht zum Teil dem Vorgehen in DIN EN 50129 (2003), nur dass in dieser Norm nicht eine Aussage zur Risikoreduktion getroffen werden muss, sondern dass durch einen Vergleich des geschätzten mit dem tolerierbaren Risiko Aussagen zur einzuhaltenden Gefährdungsrate zu treffen sind. Der Normentwurf FprEN 61508-1 (2008) lässt als Ergebnisart die Vorgabe einer notwendigen Risikoreduktion oder einer einzuhaltenden Gefährdungsrate zu.

Für das Automobilwesen kommt Jesty zu dem Schluss, dass die Vorgabe einer Risikoreduktion nicht zielführend ist. Sein Vorschlag, als Vorgabewerte Anforderungen an die zulässige Gefährdungsrate zu stellen, entspricht weitestgehend dem Vorgehen nach DIN EN 50129 (2003).

Die Verordnung EG Nr. 352/ (2009) definiert Sicherheitsanforderungen als *die (qualitativen oder quantitativen) Sicherheitsmerkmale eines Systems und dessen Betriebs (einschließlich Betriebsvorschriften), die zur Erfüllung gesetzlicher oder unternehmensspezifischer Sicherheitsziele erforderlich sind.* Sicherheitsanforderungen werden basierend auf den Ergebnissen der Risikoevaluierung abgeleitet. Wird die Risikoakzeptanz durch explizite Risikoabschätzung unter Anwendung des RAC-TS-Kriteriums durchgeführt, so ist das Ergebnis eine Ausfallrate[1].

Im Wesentlichen stehen drei Optionen für das Ergebnis einer Risikographanwendung zur Auswahl: Aussagen zur einzuhaltenden Gefährdungsrate, zur notwendigen Risikoreduktion oder zum Safety Integrity Level.

[1] In den Normen wird zumeist der Begriff der Ausfallrate verwendet. Im Kontext der Arbeit ist jedoch aufgrund der spezifizierten Definition von Gefährdung der Begriff der Gefährdungsrate zutreffender. Daher wird mit Ausnahme von Bezügen auf Normen der Begriff der Gefährdungsrate verwendet.

Wird eine zulässige Gefährdungsrate als das Ergebnis der Analyse ausgegeben, so kann mit diesem Ergebnis weitergearbeitet werden. Die Gefährdungsrate ist die Ergebnisart, die dem Anwender die meisten Möglichkeiten der Weiterverarbeitung erlaubt.

Ein Safety Integrity Level (SIL) kann nur für technische Systeme vorgegeben werden. Laut DIN EN 50129 (2003) kann aus der Kenntnis der zulässigen Gefährdungsrate ein SIL abgeleitet werden, nicht jedoch umgekehrt aus einem SIL eine zulässige Gefährdungsrate. Laut FprEN 61508-1 (2008) ist es auch möglich, aus dem SIL auf eine Gefährdungsrate zu schließen. Da eine Gefährdungsrate konkret berechnet, ein SIL jedoch immer nur durch Runden ermittelt werden kann, ist die Ableitung einer Gefährdungsrate basierend auf einem SIL potentiell ungenauer als die Ableitung des SIL ausgehend von der Gefährdungsrate.

Die Vorgabe einer Risikoreduktion ist dann sinnvoll, wenn mit dem Wert der Risikoreduktion weitergearbeitet werden soll.

Unabhängig von der obigen Diskussion kann ein Risikograph auch zur Parameter-basierten Risikoabschätzung ohne damit verbundener Anforderungsableitung genutzt werden. Ergebnis einer solchen Risikographanwendung ist ein Wert für das Risiko. Inwieweit mit diesem Wert weitergearbeitet werden kann, ist davon abhängig, wie der Risikograph konstruiert wurde. Der Wert kann dem tatsächlichem Risiko entsprechen. In diesem Fall kann mit dem Wert beliebig weitergearbeitet werden. Wurden im Risikographen Annahmen und Randbedingungen hinterlegt, die nicht quantitativ in den Risikowert einfließen, so können nur Ergebnisse, die mit dem gleichen Risikographen ermittelt wurden, miteinander verglichen werden. Eine quantitative Auswertung des Wertes außerhalb des Kontextes der Methode ist nicht möglich.

4.4 Systemmodell

Grundsätzlich ist zu unterscheiden in das einer Norm bzw. einer Risikographkonstruktion zu Grunde gelegte Systemmodell und das für eine Risikoabschätzung erstellte Risikomodell. Das Systemmodell beschreibt das grundsätzliche Zusammenwirken der funktionalen Systembestandteile, wohingegen das Risikomodell detailliert die für eine Risikoermittlung relevanten Parameter abbildet. Wesentliche, im Risikomodell zu berücksichtigende Einflüsse resultieren aus dem Systemmodell. Von den betrachteten Dokumenten trifft lediglich DIN EN 61508-1 (2002) Aussagen zum Systemmodell. Keines der Dokumente gibt konkrete Hinweise oder erhebt detaillierte Forderungen bezüglich des Risikomodells.

Das Systemmodell aus DIN EN 61508-1 (2002) ist nicht auf das Eisenbahnwesen übertragbar. Das EUC würde der „Hardware“, z.B. dem Zug und der Streckeneinrichtung entsprechen. Eine getrennte Abbildung von Steuerungseinrichtungen und Sicherungseinrichtungen wie in dem der Norm zu Grunde gelegten Systemmodell ist nicht möglich, da im Eisenbahnwesen Leit- und Steuerungssysteme immer auch Sicherheitsaufgaben haben. Nur wenige ausgewählte Systeme (z.B. die punktförmige Zugbeeinflussung) haben ausschließlich Sicherungscharakter und können als sicherheitsbezogenes System nach DIN EN 61508-1 (2002) modelliert werden. Das der Risikographerstellung zu Grunde gelegte Systemmodell und subsequent das Risikomodell müssen diese Dualität von Funktion und Sicherheitsfunktion berücksichtigen.

Die von Jesty in Jesty u. a. (2006) vertretene Argumentation für sein und gegen das Systemmodell nach DIN EN 61508 kann für das Eisenbahnwesen nur teilweise übernommen werden. Auch für das Eisenbahnwesen ist die Definition des Ablaufs vom Versagen über die Gefährdung hin zum Unfall sinnvoll. Die Aussage, dass unter der Annahme von normalem Fahren keine Gefährdungen zu erwarten sind und es daher auch kein Risiko gibt, kann nicht

nachvollzogen werden. Zum Einen sind in jedem Fall Hardware-Ausfälle zu berücksichtigen. Die Wahrscheinlichkeit von Hardware-Ausfällen kann nicht zu null reduziert werden und auch bei normalen Fahrbedingungen ggf. zu einem Unfall führen. Zum Anderen kann es durch äußere Einflüsse zu Unfällen kommen, die ggf. durch zusätzliche risikoreduzierende Maßnahmen beherrschbar sind und deshalb analysiert werden müssen.

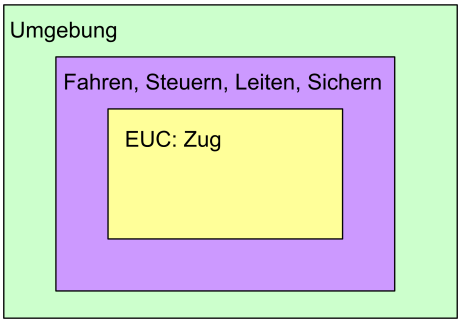

Bild 4.1: Systemmodell als Grundlage für Risikographerstellung

Als Grundlage für die weitere Arbeit ist ein Systemmodell zu erstellen. Dieses sollte gültig sein für die Risikographkonstruktion im Bereich des Eisenbahnwesens. In Anlehnung an das Modell in DIN EN 61508-1 (2002) werden die Funktionen Fahren, Leiten, Steuern und Sichern zusammengefasst. Als EUC, Equipment under Control, wird der Zug[2] als das Transportgefäß der zu transportierenden Personen und Güter gewählt. Das Wirken von Systemen zum Fahren, Leiten, Steuern und Sichern der Züge hat unmittelbaren Einfluss auf den Zug und mittelbaren Einfluss auf die im Zug beförderten Personen und Güter. Als Erweiterung des Systemmodells nach DIN EN 61508-1 (2002) wird die Umgebung als die das System umschließende Einheit formuliert. Dies hat den Zweck, den Konstrukteur einer Risikoabschätzungsmethode bereits in dieser frühen Phase der Methodenerstellung zu zwingen, Angaben zur Systemumgebung und den sich daraus ergebenden Randbedingungen zu machen.

Das abgeleitete Systemmodell ist Bild 4.1 zu entnehmen.

4.5 Analyseebene

Die Funktion eines Systems kann umfassend in wenigen oder detailierter in vielen Funktionen beschrieben werden. Im Folgenden wird es als hohe Analyseebene bezeichnet, wenn das System durch abstrakte, wenig detaillierte Funktionen beschrieben wird. Eine niedrige Analyseebene ist eine detaillierte, anwendungsnahe Systemebene. Es wird in dieser Arbeit nicht darauf eingegangen, wie Teilfunktionen der niedrigen Analyseebene aus Funktionen der höheren Ebene systematisch und möglichst vollständig abgeleitet werden können. In Kurz u. Milius (2007) wird dafür ein Verfahren vorgestellt. Grundsätzlich ist es auch vorstellbar, dass nicht die Funktionen auf unterschiedlichen Ebenen ermittelt werden, sondern die Ableitung der unterschiedlichen Ebenen für die Gefährdungen vorgenommen wird. Dieses Vorgehen erscheint jedoch weniger aussichtsreich, da es komplizierter in der Anwendung und weniger intuitiv ist, und wird deshalb nicht weiter diskutiert.

Im Rahmen der Risikographanalyse wird das von einer Gefährdung ausgehende Risiko abgeschätzt. Diese Abschätzung kann grundsätzlich auf allen Ebenen erfolgen. Die Ableitung

[2]Es wird im Folgenden der Begriff Zug für alle auf Fahrstraßen verkehrenden Fahrzeuge verwendet.

einer einzuhaltenden Gefährdungsrate ist jedoch nur möglich, wenn in der Risikoabschätzungsmethode Annahmen zur Risikoakzeptanz berücksichtigt werden. Diese Annahmen sind im Allgemeinen nur für eine definierte Ebene gültig (siehe auch Abschnitt 4.12). Deshalb muss sichergestellt sein, dass die durch die getroffenen Annahmen festgelegte Analyseebene vom Anwender eingehalten wird, d.h. die Gefährdungen auf der richtigen Ebene ermittelt werden.

Die gewählte Analyseebene entscheidet maßgeblich über die Aussagekraft und Weiterverwertbarkeit des Analyseergebnisses. Unterschiedliche Aspekte sollten deshalb berücksichtigt werden, um im Rahmen der vorgegebenen Randbedingungen die geeignete Analyseebene zu wählen. Auf diese Aspekte wird im Folgenden eingegangen.

Die Analyseebene hat Auswirkungen für die an der Analyse beteiligten Gruppen, d.h. die Eisenbahnverkehrs- und Eisenbahninfrastrukturunternehmen (EVU/EIU) und die Hersteller der Eisenbahnsicherungstechnik. Eine hohe Analyseebene bedeutet für die EVU/EIU einen geringen Aufwand bei der Funktionsdefinition. Es werden wenige Werte als Vorgabe (z. B. in Form von tolerierbaren Gefährdungsraten (*THR*)) für den Hersteller abgeleitet. Der Hersteller muss im Rahmen der Systementwicklung aus den gegebenen Funktionen die Teilfunktionen ableiten. Er hat die Möglichkeit, die Teilfunktionen nach wirtschaftlichen Aspekten zusammenzufassen und in entsprechenden Systemen zu realisieren. Dabei können die Ausfallraten für Teilfunktionen variiert werden. Es muss gezeigt werden, dass der Vorgabewert für die Funktion eingehalten wird. Da manche Teilfunktionen einfacher und preiswerter mit einer niedrigen Ausfallrate realisiert werden können als andere Teilfunktionen, kann durch Ausnutzung dieser Tatsache der Hersteller wirtschaftliche Lösungen erarbeiten. Werden diese wirtschaftlichen Lösungen auch entsprechend günstig angeboten, so ist dies ein Vorteil für den Betreiber. Da aufgrund der Designfreiheit des Herstellers die (Teil-)Systeme unterschiedlicher Hersteller nicht miteinander kombinierbar sind, bindet sich der Betreiber jedoch an einen Hersteller.

Umgekehrt bedeutet eine niedrige Systemebene einen hohen Arbeitsaufwand für den Betreiber zur Ableitung der Teilfunktionen und der zugehörigen Vorgabewerte. Die Freiheitsgrade zur Systemerstellung für den Hersteller sind eingeschränkt. Dadurch müssen u.U. unwirtschaftliche Lösungen realisiert werden. Im Gegenzug hat der Betreiber die Möglichkeit, unter den Angeboten unterschiedlicher Hersteller zu wählen und Systeme zu kombinieren.

Ebenfalls bei der Wahl der Systemebene ist zu berücksichtigen, dass, rechtlich betrachtet, die Systemverantwortung immer beim Betreiber liegt. Gibt dieser die Vorgabewerte auf niedriger Systemebene vor, muss durch ihn sichergestellt werden, dass die einzelnen Systembestandteile sicher und anforderungsgerecht zusammenwirken. Bestellt der Betreiber ein System als Komplettangebot, d.h. mit Vorgabewerten auf hoher Ebene, so kann der Betreiber vom Hersteller verlangen, dass dieser das anforderungsgerechte Zusammenwirken der Systemkomponenten garantiert.

Die Ableitung eines als tolerierbar anzusetzenden Risikos aus Statistiken ist für Funktionen auf hoher Systemebene einfacher möglich als für Teilfunktionen auf niedriger Systemebene, da im zweiten Fall oftmals zuverlässiges Zahlenmaterial fehlt, um ein solches Risiko konkret zu bestimmen.

Im Rahmen einer Risikobeurteilung erfolgt eine Gefährdungsidentifikation, in der die Gefährdungen im Allgemeinen aus den identifizierten Funktionen abgeleitet werden. Es wird davon ausgegangen, dass auf hoher Systemebene deutlich weniger Gefährdungen abgeleitet werden als auf niedriger Systemebene.

Je niedriger die gewählte Systemebene ist, desto eher ist eine Trennung von durch Mensch und Technik realisierten Funktionen möglich. Auf hoher Systemebene kann und soll zumeist

nicht unterschieden werden, ob die betrachtete Funktion durch den Menschen oder durch die Technik realisiert wird.

Wenn festgelegt wurde, welche Analyseebene die geeignete ist, so muss entschieden werden, wie die Analyseebene dem Anwender zuverlässig und unmissverständlich mitgeteilt werden kann. Die Analyseebene kann vorgegeben werden durch

- Nennung aller in Frage kommenden Funktionen oder
- eine qualitative Beschreibung der Analyseebene.

Als dritte Möglichkeit kann auf eine Vorgabe der Analyseebene verzichtet werden, wenn statt dessen (unter Einhaltung von Randbedingungen bezüglich der Risiko(gleich)verteilung) die Zahl der Gefährdungen je Funktion explizit in den Risikographen einfließt. Dieses Vorgehen würde eine maßgebliche Erweiterung der Risikographmethode bedeuten und eine Vielzahl von Annahmen und Einschränkungen notwendig machen. Ein solches Vorgehen wird zur Zeit als nicht zielführend angesehen und daher im Rahmen der Arbeit nicht betrachtet.

Wird die Analyseebene durch Vorgabe einer Funktionsliste festgelegt, so ist ein höherer Aufwand bei der Konstruktion des Risikographen zur Identifikation und Beschreibung aller Funktionen notwendig. Die Vorgehensweise hat den Vorteil, dass keine Missverständnisse bezüglich der Analyseebene möglich sind. Wenden mehrere Anwender den Risikographen an, so sind die Ergebnisse je Funktion vergleichbar. Es besteht jedoch die Möglichkeit, dass die gelisteten Funktionen nicht kompatibel sind zu den vom Anwender zu analysierenden Funktionen. In jedem Fall sollte bei Vorgabe einer Funktionsliste ein Risikobudget für weitere Funktionen des Systems berücksichtigt werden.

Wird die Analyseebene durch eine qualitative Beschreibung der Ebene vorgegeben, so sollte dies z.B. durch eine Beschreibung des Einsatzgebietes, der typischen Anforderungsart oder des Einflusses auf die Umgebung erfolgen. Eine solche Beschreibung sollte von Beispielen begleitet sein, die dem Anwender das Verständnis für die benötigte Analyseebene erleichtert. Für den Konstrukteur einer Risikoabschätzungsmethode bedeutet die qualitative Beschreibung der Analyseebene, dass er ggf. die Zahl der Gefährdungen je Funktion abschätzen muss. Der Vorteil des Vorgehens liegt in dem geringen Aufwand bei der Konstruktion, da der aufwändige Prozess, alle relevanten Funktionen zu identifizieren, entfällt. Auch besteht eine größere Flexibilität des Anwenders bei der Definition der Funktionen. Wenden mehrere Anwender den Risikographen an, so sind die Ergebnisse nicht notwendigerweise vergleichbar, da Funktionen unterschiedlich definiert und abgegrenzt sein können.

4.6 Funktionen

4.6.1 Funktion und Sicherheitsfunktion

Ausgangspunkt der Risikoabschätzung sind die Funktionen eines Systems. Der Begriff Funktion wird in DIN EN 50129 (2003) definiert als *Art von Aktion oder Tätigkeit, durch die ein Produkt seinen beabsichtigten Zweck erfüllt.* Im Zuge der Gefährdungsermittlung sind alle Funktionen bzw. deren Fehlfunktionen auf ihr Gefährdungspotential hin zu untersuchen und die identifizierten Gefährdungen sind zusammenzustellen. Es muss sichergestellt sein, dass jede Funktion unabhängig von den anderen Funktionen betrachtet werden kann. Es müssen (implizit) Schnittstellen festgelegt sein, an denen Funktionen voneinander getrennt und an die ggf. Anforderungen gestellt werden können.

Neben dem Begriff der Funktion wird häufig auch der Begriff der Sicherheitsfunktion verwendet. In DIN EN 61508-4 (2002) wird der Begriff der Sicherheitsfunktion definiert: *Funktion, die von einem E/E/PE-sicherheitsbezogenen System, einem sicherheitsbezogenen System anderer Technologie oder externen Einrichtungen zur Risikominderung ausgeführt wird mit dem Ziel, unter Berücksichtigung eines festgelegten gefährlichen Vorfalls einen sicheren Zustand für die EUC zu erreichen.* Die Definition ist nur im Kontext des Systemmodells aus DIN EN 61508-1 (2002) sinnvoll. Da das Systemmodell der DIN EN 61508-1 (2002) nicht übernommen wurde, ist eine Anpassung der Definition von Sicherheitsfunktion an die Gegebenheiten des Eisenbahnwesens notwendig. In DIN EN ISO 13849-1 (2004) wird folgende Definition von Sicherheitsfunktion gegeben: *Funktion einer Maschine, wobei ein Ausfall der Funktion zur unmittelbaren Erhöhung des Risikos (der Risiken) führen kann.* In DIN EN 50126 (2000) und DIN EN 50129 (2003) wird Sicherheitsfunktion nicht definiert. Es wird jedoch ausgeführt, dass Sicherheitsintegritätslevel dazu dienen, die ausreichende Sicherheit von Sicherheitsfunktionen zu spezifizieren bzw. die Fähigkeit beschreiben, geforderte Sicherheitsfunktionen zu erbringen. Die identifizierten Sicherheitsfunktionen sind wesentlicher Bestandteil des Sicherheitsnachweises und des Genehmigungsprozesses.

Da die in den Normen gegebenen Sicherheitsfunktionen für eine praktische Anwendung zu wenig spezifisch scheinen, werden im Rahmen der Arbeit die folgenden Optionen für die Definition von Sicherheitsfunktion diskutiert:

- Alle Funktionen, aus deren Nichterfüllung Gefährdungen (siehe Abschnitt 4.7) resultieren, werden als Sicherheitsfunktionen bezeichnet.

- Alle Funktionen, an die im Rahmen des Sicherheitsnachweises qualitative und/oder quantitative Anforderungen gestellt werden, bzw. für die im Sicherheitsnachweis Annahmen getroffen werden, werden als Sicherheitsfunktionen bezeichnet.

- Alle Funktionen, für die eine zulässige Gefährdungsrate kleiner als 10^{-5} Gefährdungen pro Stunde (SIL 1) gefordert wird, werden als Sicherheitsfunktionen bezeichnet.

Die Klassifikation aller Funktionen, die zu einer Gefährdung führen können, als Sicherheitsfunktionen ist zu wenig detailliert. Im Ergebnis einer solchen Zuweisung werden sehr viele Funktionen als Sicherheitsfunktionen bezeichnet. Damit hat diese Zuordnung wenig Aussagekraft.

Die als dritte Variante vorgestellte Möglichkeit hat den Vorteil, dass sie einen Benchmarkwert enthält und damit wenig Interpretationsspielraum lässt. Bei Anwendung dieser Definition besteht jedoch die Schwierigkeit, diejenigen Funktionen korrekt zu bezeichnen und zu erfassen, für die eine Gefährdungsrate größer als 10^{-5} Gefährdungen pro Stunde oder gar keine Gefährdungsrate gefordert wird, die jedoch einen Beitrag zur Sicherheit leisten bzw. für die im Rahmen des Sicherheitsnachweises Annahmen getroffen wurden.

Es wird vorgeschlagen, die zweite Variante als Definition für den Begriff der Sicherheitsfunktion zu verwenden.

- Durch den Begriff der Sicherheitsfunktion wird eine Trennung der Funktionen mit Sicherheitsanforderungen und der Funktionen ohne Sicherheitsanforderungen möglich. Die Verwendung des Begriffs Sicherheitsfunktion lässt keine Rückschlüsse auf die Art der Sicherheitsanforderung zu.

- Die Klassifizierung als Sicherheitsfunktion ist das Ergebnis der Risikoabschätzung bzw. Risikobeurteilung und kann nicht vor der Analyse erfolgen.
- Jede Funktion kann eine Sicherheitsfunktion sein.

Welche Anforderungen bezüglich des Genehmigungsprozesses an Sicherheitsfunktionen zu stellen sind, muss herausgearbeitet werden. Dies ist nicht Teil der vorliegenden Arbeit.

4.6.2 Stand der Technik - Beschreibung des Systems Eisenbahn durch Funktionen

Ein einfacher Weg zur Festlegung der Analyseebene des Risikographen wäre es, wenn auf bereits vorhandene funktionale Systembeschreibungen bzw. Zusammenstellungen von Systemfunktionen zurückgegriffen werden kann. Dieser Weg wurde beispielsweise in der Dissertation von Bepperling (Bepperling (2009)) gewählt. Dort wurde die in prEN 15380-4 (2007) vorgegebene Systematik erweitert und für die Anwendung im Rahmen der Methode BPrisk aufbereitet.

In der Literatur gibt es eine Vielzahl von Ansätzen der Eisenbahnsystembeschreibung. Es werden die folgenden, aus aktuellen Veröffentlichungen stammenden, Ansätze kurz vorgestellt und analysiert. Eine Bewertung der Ansätze hinsichtlich ihrer Eignung als Basis einer Risikographkonstruktion erfolgt im Abschnitt 5.6.

- Normentwurf prEN 0015380-4: Railway applications - Classification system for rail vehicles (prEN 15380-4 (2007))
- Generic Hazard List Methodology (UIC (2007))
- Rail Optimisation Safety Analysis (ROSA) (Klinge u. a. (2008))
- Realisierungsunabhängige Identifizierung von Gefährdungen auf der Basis betrieblicher Funktionen (Top-Down-Ansatz nach Bosse u. Gayen (2008))
- Systematische Beschreibung des Eisenbahnbetriebs (Top-Down-Ansatz nach Eickmann u. a. (2008))

Die in prEN 15380-4 (2007) veröffentlichte Liste beinhaltet eine Kennzeichnungssystematik für Schienenfahrzeuge. Ausgehend von wenigen übergeordneten Funktionen werden Subfunktionen auf zwei bzw. vier weiteren Ebenen abgeleitet. Die Zusammenstellung der Funktionen basiert auf den älteren Dokumenten DIN 25002 Teil 5 (Entwurf) sowie der MODTrain Struktur, welche von der Union des Industries Ferrovieaires Europeennes (UNIFE) entwickelt wurde.

Die Generic Hazard List Methodology wurde im Rahmen eines europäischen Projekts entwickelt (UIC (2007)). Im Rahmen des Projekts wurden *signalling hazards* identifiziert, d.h. Gefährdungen, die Auswirkungen auf die Funktionsweise eines Stellwerks bzw. Stellwerkkernels haben. Einerseits wurde ein funktionaler Ansatz für die Identifikation der Gefährdungen gewählt, anderseits wurde jedoch auch berücksichtigt, dass eine physische Struktur, d.h. fertige Komponenten bereits existieren und sich im Einsatz befinden. Es wurden die Versagen der Komponenten bzw. die Versagen der Kommunikation von Komponenten mit dem Stellwerk zusammengetragen. Die Gefährdung wird aus Versagen und möglichem Unfalltyp formuliert, beispielsweise *Possibility of a derailment of a railway vehicle on a moveable track element due to incorrect detected direction values of a point (left/ right).*

Das Projekt Rail Optimization Safety Analysis (ROSA), beschrieben z.B. in Klinge u. a. (2008), hat unter anderem das Ziel, für das Eisenbahnwesen Beziehungen zwischen Sicherheitszielen und Sicherheitseinrichtungen methodisch und logisch abzuleiten. Grundlage für diese Arbeit ist die Beschreibung eines *Basic System Model*, innerhalb dessen ein rudimentäres Eisenbahnsystem ohne Sicherheitseinrichtungen abgebildet wird. Aus Fehlern in diesem vereinfachten System werden die sich ergebenden Gefährdungen, die sogenannten *Starting Point Hazards*, weiterentwickelt. Es wurden 60 Starting Point Hazards beschrieben. Es handelt sich nicht um eine funktionale Systembeschreibung, sondern um eine implizite Systembeschreibung durch Gefährdungen.

In Bosse u. Gayen (2008) wird ebenfalls ein Vorgehen zur funktionalen Beschreibung des Eisenbahnbetriebs gegeben. Es werden zunächst für alle spurgeführten Systeme allgemeingültige Grundfunktionen identifiziert. Für diese Grundfunktionen werden Gefährdungen abgeleitet. In einem zweiten Schritt können für konkret zu realisierende Systeme entsprechend der betrieblichen Abläufe mehrere Grundfunktionen mit den zugehörigen Gefährdungen kombiniert werden. Es wird keine explizite Definition der für die Grundfunktionen gewählten Funktionsebene gegeben.

In Eickmann u. a. (2008) wird ein Vorgehen zur Ableitung von Funktionen und der Visualisierung dieses Funktionsgeflechts vorgestellt. Das Vorgehen beginnt mit der Formulierung von Anforderungen. Es wird ausgeführt, dass auf Basis dieser Anforderungen Funktionen formuliert werden, die in weiteren Schritten „Top-Down“ dekompositioniert werden. Es werden Unterfunktionen formuliert, die Konkretisierungen d.h. Spezialfälle der Funktionen darstellen. Es wird deutlich gemacht, dass ab einer bestimmten Ebene zur Abbildung von realisierten Systemen nicht mehr alle Unterfunktionen benötigt werden, sondern in der jeweiligen Ebene die passende Unterfunktion zu wählen ist. In dem abschließenden Anwendungsbeispiel wird aufgezeigt, wie die Abbildung von realisierten Systemen mit der Methode dazu dienen kann, Anforderungen und Randbedingungen für die Modellierung neuer Systeme abzuleiten.

4.7 Gefährdungen

4.7.1 Definition

Mit dem Risikographen werden Gefährdungen analysiert. Es ist deshalb notwendig, dass dem Anwender eine eindeutige Definition vorliegt, was unter Gefährdung zu verstehen ist. Gefährdung/Gefahr wird in den Normen unterschiedlich definiert, beispielsweise:

- DIN EN 50126: Gefahr (hazard) - *Eine physikalische Situation, die potentiell einen Schaden für den Menschen beinhaltet*
- DIN EN 50129: Gefährdung (hazard) - *Bedingung, die zu einem Unfall führen kann*
- Verordnung EG Nr. 352/ (2009): Gefährdung - *Bedingung, die zu einem Unfall führen könnte*
- DIN EN 61508-4:
  - Gefährdung (hazard): *potentielle Schadensquelle*
  - Gefährdungssituation (hazardous situation): *Umstand, durch den eine Person einer Gefährdung ausgesetzt ist.*

  - gefährlicher Vorfall (hazardous events): *Gefährdungssituation, die zu einem Schaden führt.*

- VDI/VDE 3542-1 (2000): *Der Zustand Gefahr (d.h. das Vorhandensein nicht vertretbarer Risiken) wird oft durch den Begriff Gefährdung erläutert, der die Art der möglichen Auswirkungen einer Gefahr durch Angaben über mögliche, nicht vertretbare Personen- und/oder Sachschäden beschreibt. Die Schäden und damit auch die Gefährdung können unmittelbar und/oder mittelbar bzw. direkt und/oder indirekt sein.*

Die Definitionen sind nicht eindeutig, detailliert und aussagekräftig genug, damit ein Anwender basierend auf ihnen ohne weitere formale Informationen Gefährdungen ableiten kann. Deshalb wird in den folgenden Abschnitten für die Arbeit eine anwendbare und aussagekräftige Definition abgeleitet.

Die gegebenen Definitionen verdeutlichen, dass Gefährdung direkt im Zusammenhang mit einem Schadensereignis gesehen wird. Deshalb ist zunächst zu definieren, welche Ereignisse zu einem Schaden führen können. Umgangssprachlich werden mit einem Schaden verbundene Ereignisse als Unfall bezeichnet. Dies wird durch die in DIN EN 50129 (2003) gegebene Definition bestätigt: *Unfall ist ein nicht beabsichtigtes Ereignis oder eine Reihe von Ereignissen mit der Folge von Toten, von Verletzten, des Verlustes eines Systems oder von Umweltschäden.*

Jesty hat als Basis für seine Risikobetrachtungen ein Modell definiert, in dem eine Gefährdung auf einem *failure* beruht. *Failure* wird in DIN EN 50129 (2003) übersetzt mit *Fehlfunktion* und definiert als *Abweichung vom spezifizierten Verhalten des Systems. Eine/ein Fehlfunktion/Ausfall ist die Folge einer Fehlerursache (fault) oder eines Fehlerzustandes (error) im System.* DIN EN 61508-4 (2002) übersetzt *failure* mit *Ausfall, Versagen* und definiert dies als *Beendigung der Fähigkeit einer Funktionseinheit, die eine geforderte Funktion ausführt.* Im Folgenden wird davon ausgegangen, dass Gefährdungen auf Fehlfunktionen basieren.

Eine Fehlfunktion kann entweder zur sicheren Seite oder zur unsicheren Seite erfolgen. Eine Fehlfunktion zur sicheren Seite bedeutet, dass das betroffene System in einen sicheren Zustand übergeht. Es kann nicht mehr zu einem Unfall kommen. Es ist davon auszugehen, dass die Fehlfunktion dadurch offenbart wird. Eine Fehlfunktion zur unsicheren Seite bedeutet, dass eine Situation vorliegt, die zu einem Unfall führen kann. Es muss unterschieden werden in Fehlfunktionen zur unsicheren Seite, die einen analyserelevanten Schaden zur Folge haben können und Fehlfunktionen zur unsicheren Seite, die einen nicht analyserelevanten Schaden zur Folge haben können. Analyserelevant ist jeder Schaden, der im Rahmen der Risikomodellerstellung definiert und als zu betrachten festgelegt wurde. Gefährdungen im Sinn dieser Arbeit sind Fehlfunktionen zur unsicheren Seite mit einem Potential von analyserelevantem Schaden.

4.7.2 Direkte und latente Gefährdungen

Eine Fehlfunktion kann durch ein technisches Versagen oder einen menschlichen Fehler[3] zu Stande kommen. Es sind aber auch Situationen vorstellbar, in denen zwei oder mehr technische Versagen oder menschliche Fehler zusammentreffen müssen, damit es zu einer Fehlfunktion kommt.

[3] Im Folgenden wird der Begriff Versagen für das Nichterfüllen einer Funktion durch ein technisches System und der Begriff Fehler für das Nichterfüllen einer Funktion durch einen Menschen verwendet.

- Direkte Gefährdungen sind Fehlfunktionen, die typischer Weise durch das Versagen eines Systems bzw. durch einen menschlichen Fehler bei der Funktionserfüllung auftreten. Diese Definition entspricht weitestgehend der Definition für Einzelausfall in VDI/VDE 3542-1 (2000).

- Latente Gefährdungen sind Fehlfunktionen, die durch das Zusammentreffen des Versagens eines Systems bzw. eines menschlichen Fehlers mit mindestens einem weiteren Versagen oder Fehler auftreten können. Das einzelne Versagen bzw. der einzelne Fehler ist keine Gefährdung. Es wird nicht von einer Offenbarung des einzelnen Versagens oder Fehlers vor Auftreten der Fehlfunktion ausgegangen. Die Definition für Mehrfachausfall in VDI/VDE 3542-1 (2000) entspricht nicht der Definition für latente Gefährdung.

4.7.3 Gefährdung als Zustand oder Ereignis

Gefährdungen können danach unterschieden werden, ob sie sich direkt nach ihrem Eintreten sofort technisch oder betrieblich offenbaren, oder ob sie zunächst unentdeckt bestehen bleiben können (Bild 4.2).

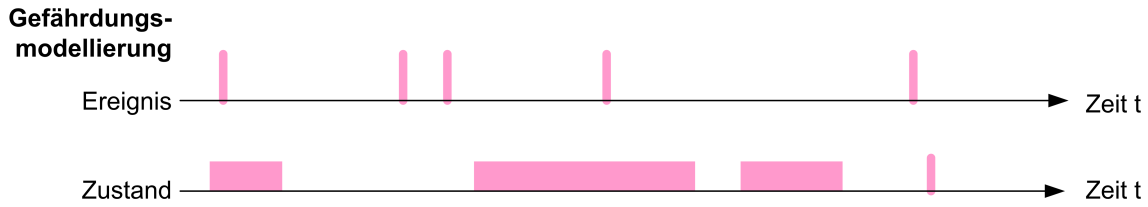

Bild 4.2: Gefährdung als Ereignis oder Zustand

Gefährdungen werden hinsichtlich der zeitlichen Abhängigkeit zwischen Auftreten der Fehlfunktion und ihrer Offenbarung als Zustand oder Ereignis bezeichnet. Es kann unterschieden werden, dass

- eine Gefährdung als Ereignis zu bezeichnen ist, wenn sie eintritt und zwingend sofort technisch oder betrieblich offenbart wird. Dies geschieht wahlweise durch ein Unfallereignis, einen Beinah-Unfall oder durch Offenbarungsmechanismen,

- eine Gefährdung als Zustand zu bezeichnen ist, wenn sie eintritt und bestehen bleibt bis es zu einem Unfall oder Beinah-Unfall kommt bzw. die Gefährdung durch Offenbarungsmaßnahmen aufgedeckt wird.

In der vorliegenden Arbeit werden Funktionen des Eisenbahnwesens betrachtet. Nicht jede Funktion wird dauerhaft-kontinuierlich beansprucht, so dass davon auszugehen ist, dass Gefährdungen bestehen können, bevor es zur Offenbarung kommt. Gefährdungen sind als Zustand zu definieren. Sollen Gefährdungen identifiziert werden, die Ereignisse sind, so können diese als Spezialfall modelliert werden.

Es ist grundsätzlich vorstellbar, dass auch ohne Offenbarung eine Gefährdung in einen sicheren Zustand zurückgesetzt wird. Dies kann der Fall sein, wenn z.B. durch Prüfmechanismen ein System regelmäßig in einen definierten Zustand überführt wird. Dieser Fall wird in der vorliegenden Arbeit nicht betrachtet.

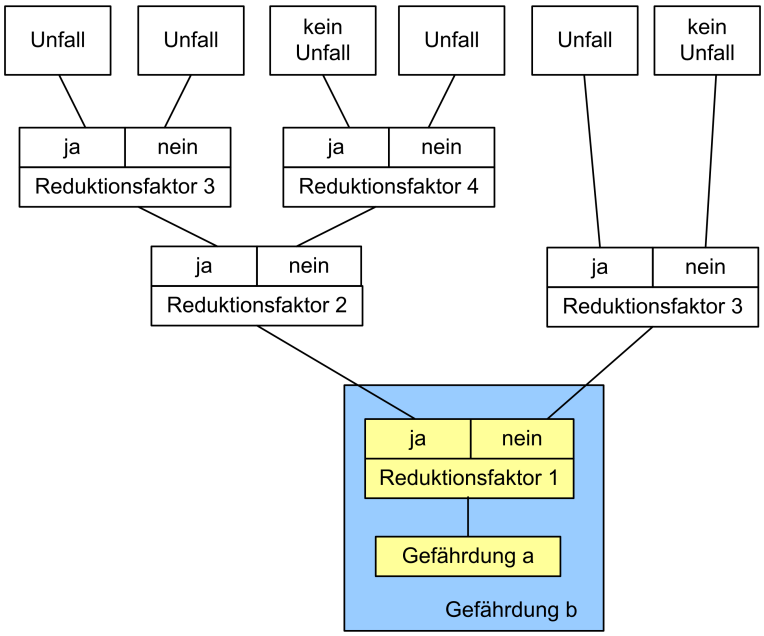

Bild 4.3: Berücksichtigung von Reduktionsfaktoren in der Gefährdungsdefinition

4.7.4 Berücksichtigung von Reduktionsfaktoren in Gefährdungen

Nicht aus jeder Gefährdung entwickelt sich ein Unfall. Die Faktoren, die über die Wahrscheinlichkeit eines Unfalls entscheiden, werden als Reduktionsfaktoren bezeichnet.

In quantitativen Analysen werden alle den Ablauf von der Gefährdung zum Unfall beeinflussenden, vom Anwender als maßgeblich angenommenen, Faktoren explizit zahlenmäßig erfasst. Inwieweit die Erfassung eines Faktors dabei im Rahmen der Gefährdungsdefinition oder der Reduktionsfaktoren geschieht, ist in der Analyse offensichtlich und weitgehend Vereinbarungssache zwischen den Analyseteilnehmern. Bei qualitativen und semi-qualitativen Analysen ist es nicht notwendigerweise offensichtlich, wo die Einflussfaktoren berücksichtigt werden. Der Konstrukteur der Methode muss eindeutig festlegen, ob dies in der Gefährdungsdefinition oder in den Parametern der Analysemethode erfolgen soll. Wird die Gefährdungsdefinition anders angewendet als vom Konstrukteur geplant, so werden Faktoren entweder gar nicht oder mehrfach in der Analyse berücksichtigt. Dies führt zu fehlerhaften Ergebnissen und muss deshalb vermieden werden. Dies illustriert Bild 4.3 am Beispiel eines Ereignisbaums. Geht der Konstrukteur von einer Gefährdungsdefinition a aus, der Anwender definiert jedoch Gefährdung b, so wird der Reduktionsfaktor 1 doppelt berücksichtigt: Einmal wie vom Konstrukter vorgesehen in einem Parameter und einmal im Rahmen der Gefährdung.

4.7.5 Ableitung von Gefährdungen

Gefährdungen sind Fehlfunktionen, d.h. sie werden aus Funktionen abgeleitet. Grundsätzlich sind dabei zwei unterschiedliche Vorgehensweisen zu unterscheiden.

Gefährdungen durch Negierung

Wird die Gefährdung durch Negierung der Funktion ermittelt, so kann nur eine gesamtheitliche Betrachtung der Funktion erfolgen. Es wird ein Vorgabewert abgeleitet, welcher durch den Hersteller des Systems bei der Umsetzung der Funktion zu realisieren ist. Ein solches Vorgehen erscheint sinnvoll, wenn alle detaillierten Gefährdungen im Wesentlichen unter gleichen Randbedingungen zu ähnlichen Folgen führen. Unterscheiden sich die Gefährdungen maßgeblich (z.B. in den potentiellen Auswirkungen), so hat das Vorgehen den Nachteil, dass bei der Risikoabschätzung der ungünstigste Fall anzunehmen ist und so potentiell zu strenge Anforderungen abgeleitet werden. Die Abschätzung der Unfallwahrscheinlichkeit ist bei Gefährdungen durch Negierung schwieriger ist als bei detaillierten Gefährdungen, da mehr und ggf. unterschiedliche Reduktionsfaktoren zu berücksichtigen sind. Das genannte Vorgehen gibt dem Hersteller, unter Berücksichtigung etwaiger anderer Vorgaben, größtmögliche Design- und Architekturfreiheit.

Wenn die Funktion aufgrund ihrer Art und ihres Umfelds eine Gefährdungsableitung durch Negierung zulässt, so sollte dieser Weg als der einfachste und am schnellsten zielführende gewählt werden.

Gefährdung durch detaillierte Ausfallbetrachtung

Die Ermittlung der Gefährdung durch Betrachtung einzelner Ausfallmodi ist sinnvoll, wenn bereits ausreichend Informationen zum Umfeld der Funktion und ihrer Interaktion mit anderen Funktionen bekannt sind. Das Vorgehen ermöglicht es, detaillierte Vorgabewerte für die einzelnen Gefährdungen abzuleiten. Die Einhaltung dieser Werte muss vom Hersteller eines entsprechenden technischen Systems gezeigt werden, was unter Umständen zu Einschränkungen beim Systemdesign bzw. der System-Architektur führen kann. Das Vorgehen kann sinnvoll sein, wenn die unterschiedlichen Gefährdungen stark voneinander abweichende Sicherheitsanforderungen stellen.

Wurden basierend auf einer Funktion unterschiedliche Gefährdungen identifiziert und analysiert, so hat der Anwender die folgenden Optionen:

- Es wird die maximal ermittelte Sicherheitsanforderung einer Gefährdung auf die Funktion bzw. das System übertragen.
- Es wird eine gewichtete Gefährdungsrate in Abhängigkeit der betrieblichen Auftretens-/Anforderungshäufigkeit ermittelt und als Sicherheitsanforderung für die Funktion bzw. das System aufgestellt.
- Es werden alle abgeleiteten Sicherheitsanforderungen für die Funktion bzw. das System zusammengestellt und einzeln nachgewiesen.

Die einfachste Vorgehensweise ist die Wahl der höchsten (Teil-)Sicherheitsanforderung als gültige für die Funktion. Eine Wichtung der Ergebnisse ist mit einem erhöhten Aufwand für die Ermittlung der benötigten Daten verbunden. Grundsätzlich muss davon ausgegangen werden, dass die benötigten Daten nicht zur Verfügung stehen und daher Expertenschätzungen herangezogen werden. Dieser Weg sollte verfolgt werden, wenn ohne eine Wichtung eine zu hohe Sicherheitsanforderung abgeleitet wird. Die Vorgabe verschiedener Gefährdungsraten ist sinnvoll, wenn der Hersteller ausreichend Designfreiheit hat.

4.7.6 Bedingungen für Gefährdungen im Risikographen

Es gibt grundsätzliche Randbedingungen die einzuhalten sind, wenn unterschiedliche Gefährdungen mit dem gleichen Riskographen analysiert werden sollen. Dazu gehören, dass

- für die zu analysierenden Funktionen und zugehörigen Gefährdungen die gleichen Normen und Richtlinien gelten müssen, da diese Grundlage der Risikoabschätzung sind,
- das abzuschätzende Risiko mit dem gleichen Risikomodell und durch die gleiche Risikoformel beschrieben werden kann,
- für die zu analysierenden Funktionen/Gefährdungen grundsätzlich das gleiche Risikoakzeptanzkriterium gilt.

4.8 Risiko im Risikographen

4.8.1 Unfallszenarien im Risikographen

Eine Funktion kann zu verschiedenen Gefährdungen führen. In Abhängigkeit der betrieblichen Situation, im Folgenden Szenario genannt, kann es zu Unfällen kommen.

In einer quantitativen Analyse werden die Parameter zur Risikoberechnung für jedes relevante Szenario einer Gefährdung ermittelt. Für jedes dieser Szenarien kann ein Risiko berechnet werden. Abschließend kann über alle Szenarien unter Berücksichtigung der Auftretenswahrscheinlichkeit der Szenarien ein Gesamtrisiko addiert werden. Dieses Vorgehen wird anhand einer Form der quantitativen Konsequenzenanalyse, dem Ereignisbaum, gezeigt. Dabei liegt der Schwerpunkt der Betrachtung auf den Parametern Schadensausmaß und Unfallwahrscheinlichkeit. Der Einfluss von Gefährdungsdauer und Aussetzungszeit wird vernachlässigt.

Die Ereignisbaumanalyse ist ein Vorgehen, mit dem die sich aus einer Gefährdung unter Berücksichtigung der Einflüsse auf die Unfallwahrscheinlichkeit ergebenden Handlungsabläufe bis zum möglichen Unfall detailliert abgebildet werden können. Jeder Zweig im Ereignisbaum entspricht einem Szenario. Jeder Zweig, der zu einem Unfall führt, trägt zum Risiko bei. Um das insgesamt von der Gefährdung ausgehende Risiko zu ermitteln, ist die Summe über alle zum Risiko beitragenden Ereignisbaumzweige zu bilden und mit der Gefährdungsrate zu multiplizieren. Bei Vorgabe eines Risikos kann eine Gefährdungsrate abgeleitet werden. Die Erstellung eines Ereignisbaums erfolgt im Allgemeinen zunächst qualitativ und dann quantitativ.

Wie das Beispiel in Bild 4.4 anschaulich zeigt, können im Ereignisbaum die unterschiedlichen, sich aus einer Gefährdung entwickelnden Szenarien berücksichtigt werden. Die Unfallwahrscheinlichkeit, ausgedrückt durch die Art, Anzahl und den quantitativen Wert der Reduktionsfaktoren, ist für jedes Szenario unterschiedlich. In qualitativen Analysen ist es nicht möglich bzw. nicht üblich, den Beitrag aller Szenarien zum Risiko zu berücksichtigen. Es erfolgt im Allgemeinen eine Vereinfachung dahingehend, dass nur ein Szenario betrachtet wird. Die Abstraktion von der Ereignisbaumdarstellung zur Erfassung im Risikographen ist grundsätzlich zulässig. Dies kann damit begründet werden, dass auch ein scheinbar detailliertes Vorgehen mit z.B. einem Ereignisbaum nur eine Vereinfachung ist, da es in der Realität unbegrenzt viele Unfallszenarien gibt. Dies wird in Tabelle 4.1 verdeutlicht.

Es muss sichergestellt sein, dass durch diese Vereinfachung nicht ein zu geringes Risiko ermittelt wird, was bedeuten würde, dass nicht die angestrebte Risikoakzeptanz gegeben ist.

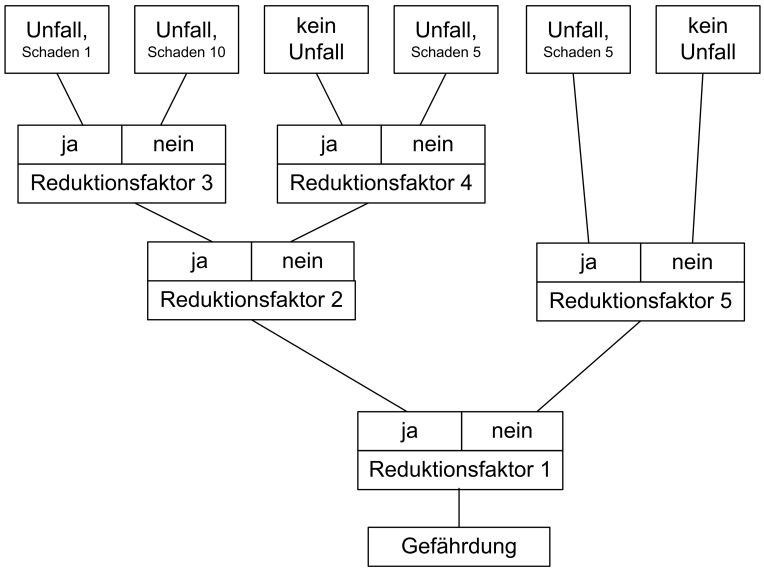

Bild 4.4: Beispiel für einen Ereignisbaum

Dies kann beispielsweise durch eine konservative Wahl der abzuschätzenden Parameter und ggf. durch Einführung eines Aufschlags auf den abgeschätzten Wert erfolgen. Wenn für eine Gefährdung sehr unterschiedliche Unfallszenarien vorstellbar sind und es nicht offensichtlich ist, welches das Maßgebliche ist, dann müssen mehrere Unfallszenarien getrennt voneinander beurteilt werden. In diesem Fall muss abgewogen werden, wie aus den ermittelten Werten Vorgabewerte abgeleitet werden können. Dies kann beispielsweise durch gewichtete Mittelwertbildung oder Wahl des konservativsten Ergebnisses erfolgen. Das beschriebene Vorgehen zum Umgang mit mehreren Szenarien einer Gefährdung entspricht weitestgehend dem Vorgehen der Berücksichtigung mehrerer Gefährdungen einer Funktion (siehe Abschnitt 4.7.5). Es ist vorstellbar, dass ein Vorgehen entwickelt wird, durch das der Risikobeitrag von mehreren Szenarien bei qualitativen Analysen, im Besonderen bei der Risikographanalyse, berücksichtigt werden kann. Eine solche Erweiterung der Risikographmethode soll hier nicht betrachtet werden.

In Bild 4.8 ist beispielhaft dargestellt, wie sich die Einzelrisiken der verschiedenen Szenarien einer Gefährdung zu einem Gesamtrisiko summieren. Für die Ermittlung des Gesamtrisikos wird davon ausgegangen, dass die Häufigkeit des virtuellen, im Risikomodell des Risikographen berücksichtigten Szenarios der Summe aus den Häufigkeiten der realen Szenarien entspricht.

4.8.2 Qualitatives Risikomodell

Das Risikomodell als Basis einer Risikographkonstruktion muss alle wesentlichen Einflüsse auf das Risiko umfassen. Die Gesamtheit des Risikomodells ergibt sich aus einer detaillierten Beschreibung des Systemmodells und aus den Anforderungen an den Risikographen.

Das qualitative Risikomodell sollte mindestens die folgenden Aspekte umfassen:

- detaillierte Beschreibung des Betrachtungsobjekts; soll das Risiko von Personen ermittelt werden, sind Aussagen zur Art der betrachteten Personengruppe und zu deren Aussetzungszeit zu treffen,

Realität • Es gibt eine beliebig große Anzahl von Szenarien, wie sich aus einer Gefährdung ein Unfall entwickelt. • Die mit jedem Szenario verknüpfte Unfallwahrscheinlichkeit ist nicht determiniert, sondern kann beliebig in Abhängigkeit der Randbedingungen variieren. • Das Unfallausmaß ist abhängig vom gewählten Szenario. Das Unfallausmaß kann stark variieren. Der Zusammenhang ist in Bild 4.5 dargestellt: Es gibt beliebig viele Szenarien, von denen vier exemplarisch dargestellt wurden. Innerhalb eines Szenarios kann sowohl die Unfallwahrscheinlichkeit, sowie in Abhängigkeit von der Unfallwahrscheinlichkeit das Schadensausmaß je Ereignis variieren.
Im Ereignisbaum erfolgt eine Abstraktion • Es sollen alle wesentlich zum Risiko beitragenden Szenarien erfasst werden. Es werden nicht alle möglichen Szenarien betrachtet, da die Zahl und Art der Reduktionsfaktoren und damit die Zahl der Szenarien beliebig groß sein kann. • Die Reduktionsfaktoren werden für jedes Szenario quantitativ festgelegt. Damit wird jedem Szenario genau eine Unfallwahrscheinlichkeit zugeordnet. • Jedem Unfall wird ein Unfallausmaß zugeordnet. Der Zusammenhang ist in Bild 4.6 dargestellt: Im Ereignisbaum wird eine begrenzte Zahl von Szenarien, hier im Beispiel vier Szenarien, betrachtet. Für jedes Szenario wird aus der Bandbreite der möglichen Werte nach festgelegten Kriterien jeweils ein Wert für die Unfallwahrscheinlichkeit und ein zugehöriger Wert für das Schadensausmaß je Ereignis gewählt. Es ist möglich, das gleiche Szenario mit unterschiedlichen quantitativen Angaben zu berücksichtigen.
Für qualitative und semi-qualitative Methoden muss eine weitere Vereinfachung erfolgen • Es wird im Allgemeinen nur ein Szenario zum Unfall betrachtet; mehrere Szenarien sind bei Weiterentwicklung der Methode u.U. möglich. • Es wird eine Unfallwahrscheinlichkeit abgeschätzt. • Es wird ein Unfallausmaß abgeschätzt. Der Zusammenhang ist in Bild 4.7 dargestellt: Es wird ein Szenario betrachtet. Im Rahmen der Analyse wird nach festgelegten Kriterien ein Wert für die Unfallwahrscheinlichkeit und ein Wert für das Schadensausmaß gewählt. Diese Werte können, müssen aber nicht aus einem Szenario stammen. Sie können auch unabhängig voneinander gewählt werden.

Tabelle 4.1: Die Abstraktion in der Abbildung der Unfallszenarien

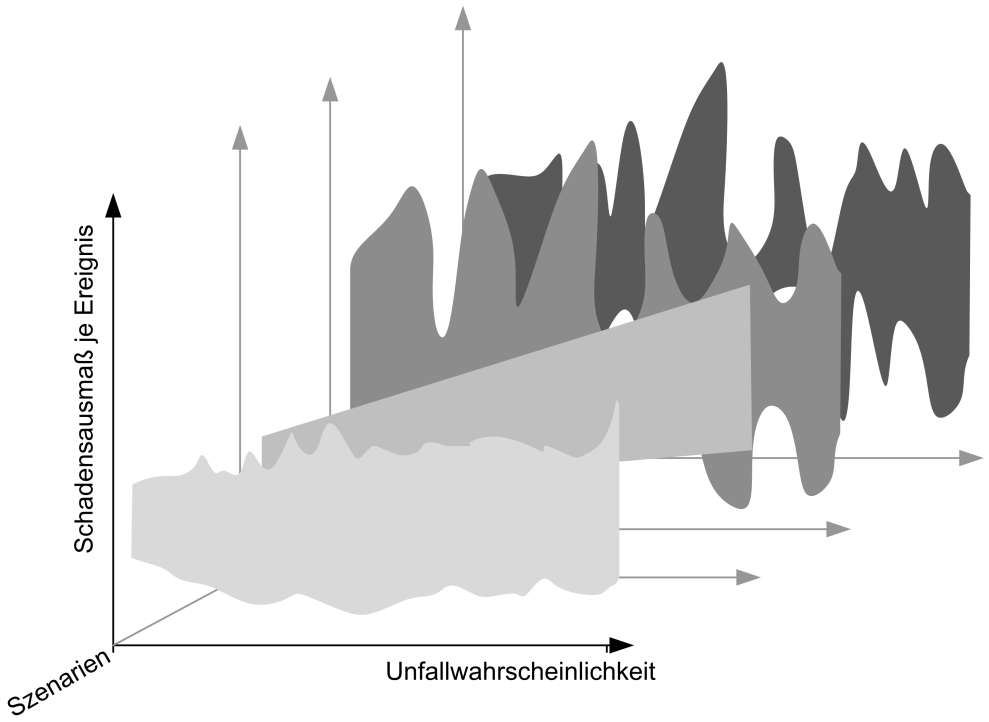

Bild 4.5: Abbildung der in der Realität möglichen Unfallszenarien

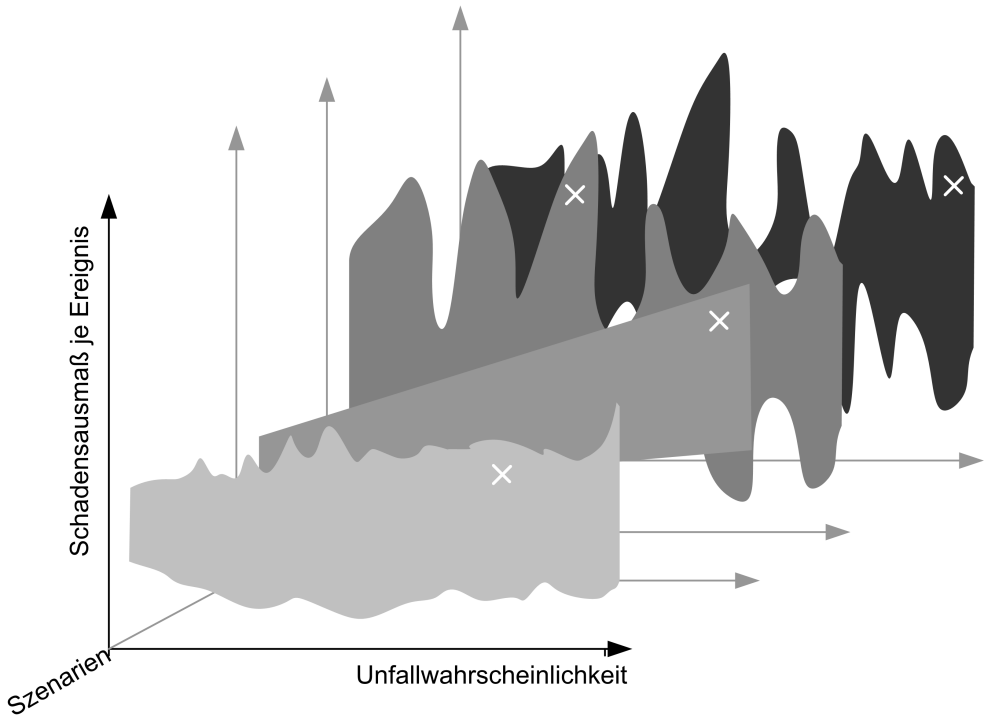

Bild 4.6: Abbildung der in einem Ereignisbaum zu berücksichtigenden Unfallszenarien (gewählte quantitative Werte durch Kreuz dargestellt)

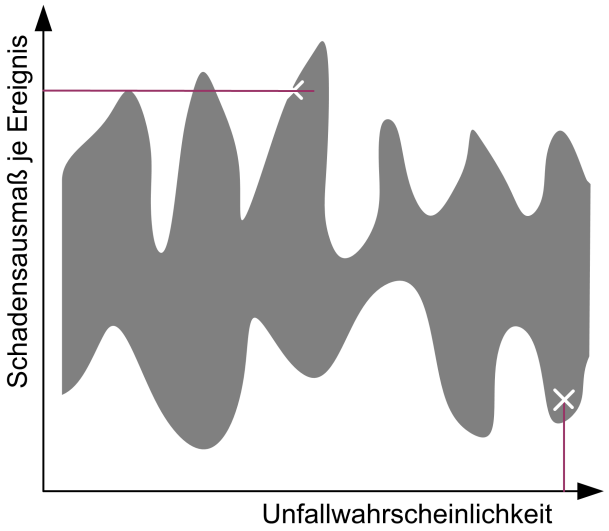

Bild 4.7: Abbildung der für einen Risikographen zu wählenden, quantitativen Werte (durch Kreuz dargestellt) innerhalb eines Szenarios

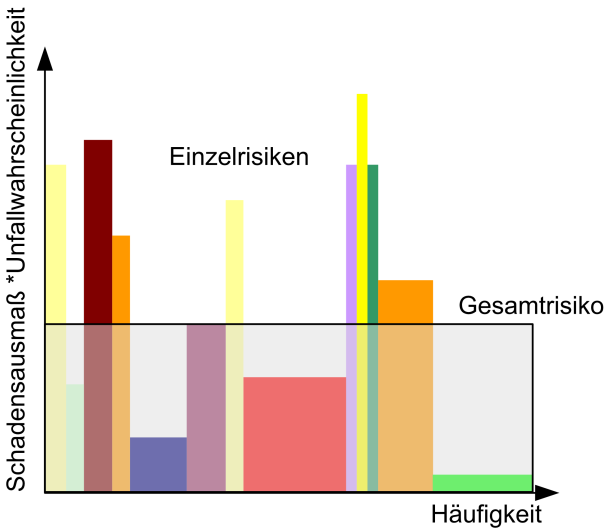

Bild 4.8: Das Gesamtrisiko setzt sich aus vielen Einzelrisiken zusammen

- Beschreibung der Wirkungsweise der Funktionen,
- Beschreibung des Bezugsobjekts,
- Beschreibung des zu betrachtenden betrieblichen Szenarios.

4.8.3 Risikoformel

Basierend auf dem Risikomodell ist eine Formel zur mathematischen Beschreibung von Risiko abzuleiten, bzw. eine bereits existierende Formel anzupassen. Diese Formel kann entweder direkt in einen Risikographen umgesetzt werden oder es ist eine Abstraktion notwendig. Es ist davon auszugehen, dass die Risikoformel im Allgemeinen zu kompliziert ist und daher eine Vereinfachung notwendig wird.

Basierend auf der Definition von Risiko kann im einfachsten Fall Risiko berechnet werden als das Produkt aus einem Erwartungswert für das Schadensausmaß und der Schadensrate. In den meisten Fällen sind die benötigten Zahlenwerte jedoch nicht direkt verfügbar. So kann die Schadensrate zusammengesetzt werden z.B. aus der Gefährdungsrate und der Unfallwahrscheinlichkeit. Gegebenenfalls muss noch die Gefährdungsdauer und/oder die Aussetzungsdauer der betrachteten Personen berücksichtigt werden. Ziel der Risikoabschätzung ist es, zu zeigen, welche Anforderungen an eine Funktion zu stellen sind, damit das von dieser Funktion ausgehende Risiko tolerierbar ist. Bei der Beurteilung von latenten Gefährdungen ist ggf. ein zusätzlicher Arbeitsschritt vorzusehen, der die Aufteilung des Ergebnisses auf alle beteiligten Systeme bzw. Personen erlaubt.

Erfolgt die Kalibrierung des Risikographen anhand eines Risikowerts, so muss das mit dem Risikographen ermittelte Risiko in Art und Bezugsgröße zum vorgegebenen Risikowert passen. Wenn ein multiplikativer Zusammenhang angenommen wird, kann das tolerierbare Risiko R_{tol} als Produkt aus einer Funktion f mit den Parametern X_1 bis X_n und der tolerierbaren Gefährdungsrate THR wie folgt dargestellt werden:

$$R_{tol} = THR \cdot f(X_1, .., X_n) \tag{4.1}$$

$$THR = \frac{R_{tol}}{f(X_1, .., X_n)} \tag{4.2}$$

Wenn die tolerierbare Gefährdungsrate das Ergebnis der Analyse und das tolerierbare Risiko eine Eingangsgröße ist, so muss der Risikograph den Term $f(X_1, .., X_n)$ abbilden. Es müssen nicht alle Parameter explizit durch den Anwender angegeben werden, sondern es ist auch möglich, für einige Parameter begründete Annahmen zu treffen und in die Konstruktion als Konstanten einfließen zu lassen.

Um das insgesamt von einer Funktion ausgehende Risiko abzuschätzen, müssen alle Schadensarten berücksichtigt werden. Dies ist nicht immer möglich bzw. nicht erwünscht. Die bisher im Eisenbahnwesen durchgeführten Risikoanalysen haben im Allgemeinen das individuelle Risiko (eines Reisenden) analysiert, d.h. einen Personenschaden betrachtet. Dieses Vorgehen orientiert sich an den Aussagen im Kommentar zur EBO (Thoma u.a. (1996)), wie in Abschnitt 2.3.2 ausgeführt. Die direkte Abschätzung eines individuellen Risikos ist unter Umständen in einer semi-qualitativen Analyse schwierig, da Aussagen zu einer Einzelperson wenig intuitiv sind. Im Unterschied zum individuellen Risiko kann auch ein kollektives Risiko ermittelt werden, wenn ein Personenkollektiv, z.B. alle Insassen eines Zuges, betrachtet wird.

Eine Risikoformel, die detailliert das individuelle Risiko abbildet, wurde von Braband entwickelt. Zur Berechnung eines individuellen Risikos aus technischen Systemen (in der Einheit Opfer[4] pro Individuum pro Jahr) kann die folgende Formel herangezogen werden:

$$IRF_i = N_i \sum_{Gefährd.H_j} (HR_j \cdot D_j + HR_j \cdot E_{ij}) \sum_{UnfälleA_k} C_{jk} \cdot F_{ik} \tag{4.3}$$

Darin bedeuten die Formelzeichen

- IRF_i Individuelles Risiko einer Bezugsperson in Opfer je Individuum und Zeiteinheit
- N_i Nutzungsprofil der Person i
- H_j Gefährdung j
- HR_j Gefährdungsrate der Gefährdung j
- D_j Betriebliche Dauer der Gefährdung j
- E_{ij} Aussetzungsdauer der betrachteten Person i der Gefährdung j
- A_k Unfallart k
- C_{jk} Wahrscheinlichkeit, dass die Gefährdung j zu einem Unfall k führt
- F_{ik} Wahrscheinlichkeit, dass die betrachtete Person i beim Unfall k zu Tode kommt

Bei der Anwendung der Formel wird davon ausgegangen, dass ein Individuum einem System ausgesetzt ist, welches durch technisches Versagen Gefährdungen produziert. Es wird das Risiko über alle von dem System ausgehenden Gefährdungen ermittelt. Die Gefährdungen sind durch Gefährdungsraten charakterisiert. Der Faktor N beschreibt das Nutzungsprofil des betrachteten Individuums. Die Angabe des Nutzungsprofils kann umgangen werden, wenn die gesamte Formel durch die Gesamtzeit der Systembenutzung pro Jahr geteilt wird (siehe z.B. Braband u. Lennartz (2000)). Die Wahrscheinlichkeit, dass ein Individuum einer Gefährdung ausgesetzt ist, ist abhängig von der Latenzzeit D der Gefährdung (der Zeit, welche die Gefährdung besteht) und der Zeit E, welche das Individuum der Gefährdung ausgesetzt ist. Aus jeder Gefährdung können ein oder mehrere Unfalltypen A mit unterschiedlichen Folgen F resultieren. Die Wahrscheinlichkeit, dass es zu einem Unfall kommt, wird durch Reduktionsfaktoren C beschrieben. Detaillierte Informationen zur Anwendung der Risikoformel und zur Erweiterung der Risikoformel können beispielsweise in CENELEC (1999), Braband (2005) oder Braband u. Lennartz (2000) gefunden werden.

Im Rahmen einer Risikoabschätzung mit Risikographen kann stets nur eine Gefährdung und ein aus dieser Gefährdung resultierender Unfall beurteilt werden. Dies bedeutet für die Implementierung der Risikoformel im Risikographen, dass keine Summenformeln zu berücksichtigen sind. Die vorgestellte Risikoformel kann vereinfacht werden zu

$$IRF_i = N_i \cdot (HR \cdot D + HR \cdot E_i) \cdot (C \cdot F_i) \tag{4.4}$$

$$IRF_i = N_i \cdot (HR \cdot (D + E_i)) \cdot (C \cdot F_i) \tag{4.5}$$

$$IRF_{i,h} = (HR \cdot (D + E_i)) \cdot (C \cdot F_i) \tag{4.6}$$

[4]Es werden unterschiedliche Begriffe für die Einheit des Gesamtschadens verwendet. Neben dem Begriff Opfer u.a. auch equivalente Opfer und Todesfälle.

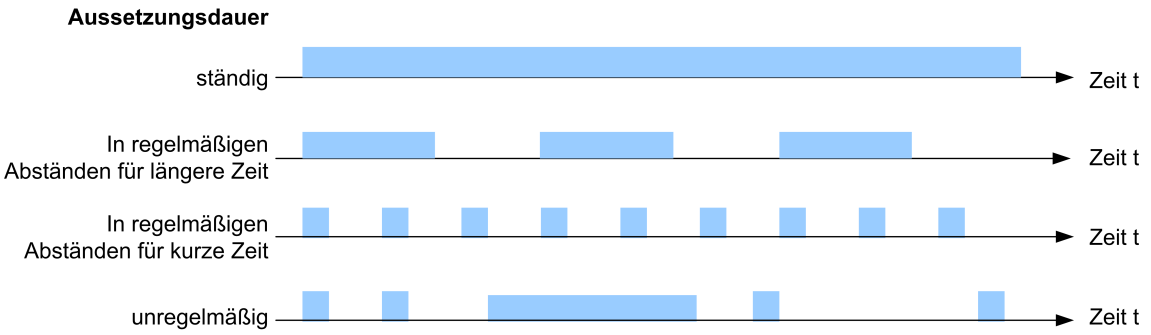

Bild 4.9: Aussetzungsdauer von schutzbedürftigen Personen

mit HR der Gefährdungsrate, D der betrieblichen Dauer der Gefährdung, der Zeit E_i, der das betrachtete Individuum i der Gefährdung ausgesetzt ist, der Wahrscheinlichkeit C, dass es zu einem Unfall kommt sowie der Wahrscheinlichkeit F_i, dass die betrachtete Person zu Tode kommt.

Können mehrere unterschiedliche Unfallarten aus einer Gefährdung erwachsen bzw. tragen mehrere Gefährdungen zum Risiko einer Funktion bei, so müssen Annahmen getroffen werden bzw. muss die Risikoabschätzung mit dem Risikographen mehrfach durchgeführt werden.

Soll kein individuelles Risiko berechnet werden, sondern ein kollektives Risiko (collective risk of fatality CRF), so muss die Risikoformel entsprechend angepasst werden. In Kurz (2007) sind erste Überlegungen zur Anpassung der Formel gegeben. Folgende Argumentation wird dort der Umwandlung der Formel zu Grunde gelegt:

- Der Betrachtungszeitraum ist eine Betriebsstunde, d.h. es wird davon ausgegangen, dass beispielsweise ein Zug eine Stunde auf der Infrastruktur unterwegs ist.
- Die Gefährdungsdauer D ist abhängig von der Art der Gefährdung und betrieblichen wie auch technischen Randbedingungen. Der Parameter D ist unabhängig von der zu ermittelnden Risikoart, da davon ausgegangen wird, dass sich die betrachteten Personen während der gesamten Betrachtungszeit im Zug befinden.
- Die Aussetzungsdauer E ist abhängig von der Art der Gefährdung. Im Besonderen ist zu berücksichtigen, dass die Gefährdungsaussetzungszeit E nicht gleichzusetzen ist mit dem Betrachtungszeitraum. Diese Annahme gilt nur für Gefährdungen von denjenigen Funktionen, die während des gesamten Betrachtungszeitraum in Anspruch genommen werden bzw. wenn das System, welches bei der Festlegung des Bezugswertes zu Grunde gelegt wird, betrachtet wird. Wird ein Teilsystem betrachtet (bzw. die Realisierung einer Teilfunktion), so kann E kleiner als der Betrachtungszeitraum sein.
- Die Unfallwahrscheinlichkeit C ist unabhängig von der Risikoart.
- Die Angabe des Schadensausmaßes F ist abhängig von der Risikoart und vom Betrachtungsobjekt, d.h. im Eisenbahnwesen beispielsweise zugbezogen.

Die bereits vereinfachte Formel zur Berechnung eines individuellen Risikos im Rahmen der Risikographkonstruktion kann in die folgende Formel zur Berechnung eines kollektiven Risikos CRF überführt werden:

$$CRF = (HR \cdot D + HR \cdot E) \cdot (C \cdot F) \tag{4.7}$$

$$CRF = HR \cdot (D + E) \cdot (C \cdot F) \tag{4.8}$$

Die Einheiten der zum kollektiven Risiko beitragenden Faktoren sind Gefährdungen je Stunde für die Gefährdungsrate, Stunde für D und E, die einheitslose Angabe Unfälle je Gefährdung für C sowie die Angabe Opfer je Unfall für den Schaden. Daraus ergibt sich die Einheit für das Risiko zu Opfer je betrachteter Bezugsgröße (z.B. Zeiteinheit).

$$[\text{Opfer}] = \left[\frac{\text{Gefaehrdung}}{\text{h}}\right] \cdot [\text{h}] \cdot \left[\frac{\text{Unfall}}{\text{Gefaehrdung}}\right] \cdot \left[\frac{\text{Opfer}}{\text{Unfall}}\right] \tag{4.9}$$

Für die Anwendung im Risikographen muss die angegebene Formel für *IRF* bzw. *CRF* vereinfacht werden. Da im Risikographen nur multiplikativ verknüpfte Parameter abgebildet werden können, gehen Aussetzungszeit und Gefährdungsdauer nicht als einzelne Parameter direkt in den Risikographen ein, sondern werden in einem gemeinsamen Parameter *DE* betrachtet. Die vereinfachte Formel zur Ermittlung des Risikos R im Risikographen ergibt sich zu

$$R = HR \cdot DE \cdot C \cdot F \tag{4.10}$$

mit *HR* der Gefährdungsrate, *DE* dem Parameter zur Abbildung von Aussetzungsdauer und Gefährdungsdauer, der Unfallwahrscheinlichkeit C sowie dem Schadensausmaß F.

Es wird davon ausgegangen, dass nur wenn alle Parameter der Risikoformel im Risikomodell berücksichtigt sind, das Modell das Risiko korrekt abbilden kann. Es ist zu unterscheiden in variable Größen, die durch den Anwender des Risikographen im Rahmen der Analyse zu wählen sind, und konstante Größen, die im Rahmen der Risikographkonstruktion gewählt wurden und unveränderlich in den Risikographen eingehen. Jeder Faktor, der zur Berechnung des Risikos im Risikographen benötigt wird, wird im Folgenden als Parameter bezeichnet. Zu jedem variablen Parameter werden mehrere Klassen definiert, die die gesamte Bandbreite an von diesem Parameter möglichen Werten abdecken. Es wird im Weiteren zunächst auf die Unterscheidung nach individuellem und kollektivem Risiko verzichtet, da eine Entscheidung, welche Risikoart zu ermitteln ist, erst mit Erstellung des Risikomodells zu treffen ist. Die grundsätzlichen Überlegungen sind unabhängig von der Risikoart.

4.8.4 Bezugsgröße des Risikos

Die Aussagekraft des Risikos ist abhängig von der gewählten Bezugsgröße. Für Systeme des Verkehrswesens kann unterschieden werden in systemunabhängige und systemabhängige Bezugsgrößen.

Als Bezugsgröße kann eine systemunabhängige, für das betrachtete Bezugsobjekt charkteristische Größe gewählt werden. Wenn beispielsweise Personenschaden analysiert wird, kann die durchschnittliche Lebensdauer der Person als Bezugsgröße gewählt werden. Dies hat den Nachteil, dass sehr seltene, bzw. kurzzeitig genutzte Systeme ein verhältnismäßig höheres Risiko tragen dürfen als häufig bzw. langandauernd genutzte Systeme. Ein solches Vorgehen bedeutet auch, dass die angenommene Nutzungszeit regelmäßig überprüft werden muss und bei einer Verlängerung der Nutzungszeit ggf. eine Anpassung der Analyse und unter Umständen des Systems notwendig wird. Wird eine systemabhängige Bezugsgröße gewählt, z.B. die

Aussetzungszeit, so ist das Risiko unabhängig von der Dauer und Art der Benutzung. Da die Nachteile bei einer systemunabhängigen Bezugsgröße überwiegen, wurde im Eisenbahnwesen in der Vergangenheit (siehe z.B. Braband u. a. (2001)) im Allgemeinen eine systemabhängige Bezugsgröße gewählt.

Eine weitere Unterscheidung, besonders für das Eisenbahnwesen von Bedeutung, ist die Unterscheidung der systemabhängigen Bezugsgrößen Kilometer und Stunde. Eine detaillierte Betrachtung dieser beiden Werte erfolgt beispielsweise in Krebs u. a. (2000). Die Vor- und Nachteile der Bezugsgrößen sind bei der Ermittlung des Risikos, im Besonderen bei der quantitativen Beschreibung der Schadensrate, zu berücksichtigen.

4.8.5 Parameterklassen

Aufgrund des angenommenen mathematischen Zusammenhangs für das Risiko hat der für die Parameterklassengrenzen gewählte Abstand maßgebliche Auswirkungen auf das erzielbare Ergebnis. Es wird betrachtet, welche Auswirkungen es auf die Ergebnisse hat, wenn der Abstand zwischen den Parameterklassengrenzen unterschiedlicher Parameter gleich oder verschieden ist. Beispielhaft wird davon ausgegangen, dass zur Berechnung des Risikos R zwei Parameter X und Y beurteilt werden müssen. Die Gefährdungsrate HR geht direkt in das Produkt ein. Alle anderen Einflüsse auf das Risiko wurden unveränderlich im Rahmen der Risikographkonstruktion festgelegt und sind im konstanten, unveränderlichen Faktor Co zusammengefasst.

$$R = HR \cdot Co \cdot X \cdot Y \tag{4.11}$$

Es wird im Risikographen ein tolerierbares Risiko R_{tol} hinterlegt, wodurch in Abhängigkeit der gewählten Parameterklassenkombination eine zulässige Gefährdungsrate HR berechnet werden kann.

$$HR = \frac{R_{tol}}{Co \cdot X \cdot Y} \tag{4.12}$$

Die Klassengrenzen des Parameters X lassen sich berechnen zu $n^e x$ mit $e = 0, 1, ...$ Die Klassengrenzen des Parameters Y lassen sich berechnen zu $m^d y$ mit $d = 0, 1, ...$ n und m sind im Folgenden die Basiswerte für die Ermittlung der Parameterklassengrenzen. x und y sind die Parameterklassengrenzwerte, die als Ausgangswerte für die Ermittlung der weiteren Klassengrenzen dienen.

Ist $n \neq m$, so variiert in Abhängigkeit von e und f der Abstand zwischen den für HR zu berechnenden Werten.

$$\text{Mit} \quad X = n^e x \quad \text{und} \quad Y = m^d y \tag{4.13}$$

$$HR = \frac{R_{tol}}{Co \cdot n^e x \cdot m^d y} \tag{4.14}$$

$$HR = \frac{R_{tol}}{xy \cdot Co \cdot n^e m^d} \tag{4.15}$$

$$HR = \frac{R_{tol}}{xy \cdot Co} \cdot \frac{1}{n^e m^d} \tag{4.16}$$

	$n \neq m$			$n = m$		
e,f	n = 10	m = 2	$n \cdot m$	n = 10	m = 10	$n \cdot m$
1,1	10	2	20	10	10	100
1,2	10	4	40	10	100	1000
2,1	100	2	200	100	10	1000
2,2	100	4	400	100	100	10000
3,2	1000	4	4000	1000	100	100000

Tabelle 4.2: Die Auswirkungen unterschiedlicher Basiswerte auf die Parameterklassenberechnung

Ist $n = m$, so beträgt der Abstand zwischen den für *HR* zu berechnenden Werten jeweils eine Potenz von n.

$$\text{Mit} \quad X = n^e x \quad \text{und} \quad Y = n^d y \tag{4.17}$$

$$HR = \frac{R_{tol}}{Co \cdot n^e x \cdot n^d y} \tag{4.18}$$

$$HR = \frac{R_{tol}}{xy \cdot Co \cdot n^{e+d}} \tag{4.19}$$

$$HR = \frac{R_{tol}}{xy \cdot Co} \cdot \frac{1}{n^{e+d}} \tag{4.20}$$

Zur Veranschaulichung der Auswirkungen werden in Tabelle 4.2 beispielhaft Werte berechnet. Da $\frac{R_{tol}}{xy \cdot Co}$ innerhalb eines Risikographen konstant ist, ist es ausreichend, zur Veranschaulichung der Auswirkungen auf die zu ermittelnde Gefährdungsrate *HR* die variablen Werte zur Berechnung heranzuziehen. Während bei $n \neq m$ der Abstand der berechneten Produkte aus n und m variiert (es treten die Faktoren 2, 5 und 10 auf), liegt bei $n = m$ stets der Faktor 10 (bzw. eine Potenz von 10) zwischen den Produkten aus n und m.

Für den Risikographen bedeutet das, dass, wenn unterschiedliche Basiswerte zur Ermittlung der Klassengrenzen der verschiedenen Parameter genutzt werden, sich zwischen den mit unterschiedlichen Parameterklassenkombinationen ermittelten Ergebnissen kein gleichmäßiger Abstand einstellt. Die Parameter haben ein unterschiedliches Gewicht auf das Endergebnis und eine systematische Ergebnisableitung ist nicht möglich.

Wenn als Basis für die Ermittlung der Parameterklassengrenzen unterschiedliche Potenzen des gleichen Wertes (z.B. bei einem Parameter werden die Parameterklassengrenzen mit n ermittelt und bei einem zweiten Parameter mit n^2) genutzt werden, so haben die Parameter ebenfalls ein unterschiedliches Gewicht auf das Endergebnis. Die Veränderung eines Parameters um eine Klasse führt nicht notwendigerweise auch zur Veränderung des Ergebnisses um eine Klasse, sondern u.U. um zwei oder mehr Klassen. Dies erlaubt dennoch eine systematische Ergebnisableitung.

Die von den Parameterklassen abgedeckte Bandbreite an Werten sollte sich an den zu erwartenden Ergebnissen bzw. den Vorgaben in maßgeblichen Richtlinien und Normen orientieren. So kann im Eisenbahnwesen bereits bei einer geringen Opferzahl von einem katastrophalen Ereignis gesprochen werden. Deshalb sollte z.B. die oberste Schadensklasse im Bereich weniger Opfer beginnen. Ein weiteres Kriterium, welches bei der Festlegung des von einem Parameter abgedeckten Wertebreichs berücksichtigt werden muss, ist die Bandbreite und der Detaillierungsgrad des Ergebnisses. Es muss sichergestellt sein, dass der Detaillierungsgrad

der Parameterklassen ausreichend ist, um bei einer risikomodellkonformen Verknüpfung der Parameter die Ergebnisbandbreite im gewünschten Detaillierungsgrad abzudecken.

Bei einer qualitativen oder semi-qualitativen Methode muss der Abstand der Klassengrenzen so gewählt werden, dass der Anwender Gefährdungen einfach zuordnen kann. Ist der Abstand zwischen den Klassengrenzen zu gering, kann der Anwender den Parameter nicht zuverlässig beurteilen. Es ist nicht zielführend, wenn beispielsweise der Schaden von Reisenden durch ein Eisenbahnunglück in eng begrenzten Klassen (z.B. Klassengrenzen 1, 2, 3 Opfer) abzuschätzen ist.

Üblicherweise werden die Parameterklassen in Tabellen zur Verfügung gestellt. In diesen Tabellen erfolgt die Zuordnung der Beschreibung der Parameterklasse zu einem Parameterklassenkürzel. Die Beschreibung der Parameterklassen ist textuell; das Kürzel ist entweder eine Kombination aus Buchstabe und Zahl oder nur eine Zahl. Das Vorgehen ist nicht immer zielführend. So ist die eindeutige Beschreibung der Klassen schwierig. Es kommt leicht zu Missverständnissen. Ein anderes Vorgehen ist denkbar. In einem Diagramm werden auf den Achsen der bzw. die wesentlichen Einflüsse auf den Parameter abgebildet. Durch Setzen des passenden Diagrammpunkts kann im Diagramm abgelesen werden, welche Parameterklasse zu wählen ist.

4.9 Optionen für das Schadensausmaß

4.9.1 Einleitung

Grundsätzlich kann die Schadensschätzung und Risikoermittlung für jede Art von Schaden erfolgen. Es ist jedoch schwierig, unterschiedliche Schadensarten gemeinsam in einem Parameter zu berücksichtigen. Daher wurde in der Vergangenheit im Allgemeinen darauf verzichtet und es wurde eine maßgebliche Schadensart betrachtet.

Es wird im Folgenden davon ausgegangen, dass Personenschaden betrachtet wird. Der Schutz des menschlichen Lebens wird für den Nachweis der Sicherheit als maßgeblich angenommen. Da in der Vergangenheit im Eisenbahnwesen die Sicherheitsnachweise unter Berücksichtigung von Personenschaden durchgeführt wurden, gibt es eine Vielzahl von Literatur, die unterstützend herangezogen werden kann. Wesentliche Grundlagen (z.B. Risikoformel) wurden explizit für das Risiko von Personenschaden hergeleitet. Die Berücksichtigung von z.B. Sachschaden und Umweltschaden erscheint dann angeraten, wenn Systeme bzw. Funktionen analysiert werden, bei denen ein Personenschaden weitgehend ausgeschlossen ist.

Es werden die verschiedenen Optionen für unterschiedliche Aspekte von Personenschaden zusammengestellt und diskutiert. Die folgende Diskussion der Parameter und Randbedingungen gilt grundsätzlich auch für eine Risikoabschätzung mit z.B. Sach- oder Umweltschaden. Allerdings sind die entsprechenden Formeln anzupassen und die formulierten Randbedingungen und Anforderungen angemessen zu übertragen bzw. zu interpretieren.

4.9.2 Schadenshöhe

Grundsätzlich sind die folgenden Optionen für den in der Analyse anzunehmenden Schaden zu unterscheiden und zu diskutieren:

1. Schaden im worst-case-Fall (denkbar höchster Schaden),
2. hohe, tatsächlich im normalen Betrieb zu erwartende Schadenshöhe,

3. mittlere Schadenshöhe,

4. am häufigsten vorkommende Schadenshöhe.

In vielen Analysen wird für die Beurteilung des zu erwartenden Schadens der worst-case-Fall betrachtet, d.h. der größte zu erwartende Schaden. Dies kann zu einem zu konservativen Ergebnis führen, wenn nicht die Unfallwahrscheinlichkeit angemessen in die Betrachtung einfließt. Erfahrungen haben gezeigt, dass bei Betrachtungen des worst-case-Falls hohe Kreativität gezeigt wird, so dass in vielen Fällen (unrealistisch) hohe Schäden ermittelt werden. Deshalb erscheint der worst-case-Fall für die Schadensermittlung zwar grundsätzlich geeignet, kann jedoch in der Anwendung zu Problemen führen.

Die Ermittlung einer hohen, im realen Betrieb unter sinnvollen Randbedingungen zu erwartenden Schadenshöhe erscheint sinnvoll. Es werden übertrieben konservative Schätzungen vermieden, aber es wird dennoch ein bedeutender, für die Gefährdung charakteristischer Schaden ermittelt. Die Ermittlung des Werts kann sowohl qualitativ durch z.B. Expertenschätzungen oder quantitativ durch Auswertung von Statistiken erfolgen.

Die Schätzung einer mittleren Schadenshöhe ist schwierig, da eine solche nicht intuitiv aus z.B. den betrieblichen Randbedingungen abgeleitet werden kann und wenig anschaulich ist.

Die häufigste Schadenshöhe ist im Allgemeinen eine sehr niedrige Schadenshöhe, die keine Aussage darüber zulässt, welches Schadenspotential eine Gefährdung tatsächlich hat.

Es wird empfohlen, eine hohe, im realen Betrieb unter sinnvollen Randbedingungen zu erwartende Schadenshöhe für den Risikographen abzuschätzen. Ein solcher Wert ist ein sinnvoller Maßstab für das tatsächlich von der Gefährdung ausgehende Risiko und in der praktischen Anwendung relativ einfach und nachvollziehbar.

4.9.3 Einflüsse auf die Schadensschätzung

Das Risiko kann als kollektives oder individuelles Risiko ermittelt werden. Unabhängig davon ist die Art der Schadensschätzung, da kollektives und individuelles Risiko, bzw. kollektiver und individueller Schaden ineinander umgerechnet werden können. Die Abschätzung des Schadensausmaßes sollte zunächst für das Kollektiv der betrachteten Personengruppe erfolgen. Der Anwender sollte einen kollektiven Schaden und nicht einen individuellen Schaden abschätzen, da das Schätzen von individuellem Schaden weniger intuitiv und nicht anschaulich ist.

Es ist festzulegen, welche Personen, bzw. welche Personengruppen betrachtet werden. In der Risikoanalyse FFB (Braband u. a. (2001)) wurde argumentiert, dass durch den Schutz der Reisenden, d.h. durch die Beschränkung des Reisendenrisikos, andere betroffene Personengruppen (Dritte, Mitarbeiter) ebenfalls ausreichend geschützt sind.

4.9.4 Der Gesamtschaden

Zur Berechnung eines Gesamtschadens mit der Einheit Opfer (auch äquivalente Opfer, englisch: equivalent fatalities) wurde in bisherigen Risikoanalysen (z.B. Risikoanalyse FFB (Günther u. a. (2001))) die Formel

$$\text{Opfer} = \text{Tote} + \frac{\text{Schwerverletzte}}{10} + \frac{\text{Leichtverletzte}}{100} \tag{4.21}$$

angewendet. In Großbritannien werden die Leichtverletzten nur mit dem Faktor 0,005 an Stelle von 0,01 berücksichtigt. Es ist keine Veröffentlichung bekannt, in der eine Begründung für den vorgestellten Zusammenhang gegeben wird.

In den europäischen Normen (z.B. DIN EN 50126 (2000)) werden zwar die Begriffe Toter und Schwerverletzter verwendet, eine Definition fehlt jedoch.

Zur Erstellung der europäischen Unfallstatistik erwartet die European Railway Agency (ERA) die Zulieferung der relevanten Daten durch die Mitgliedsländer (Verordnung EG Nr. 91/ (2003)). Dafür unterscheidet die ERA in *getötete Personen* und *schwer verletzte Personen* und gibt die folgenden Definitionen (Verordnung EG Nr. 1192/ (2003)):

- getötete Person (*person killed*): *alle Personen, die entweder unmittelbar nach einem Unfall oder innerhalb von 30 Tagen an den Unfallfolgen sterben — mit Ausnahme der Personen, die Selbstmord begangen haben;*

- schwer verletzte Person (*person seriously injured*): *alle Verletzten, die nach einem Unfall für mehr als 24 Stunden in ein Krankenhaus eingewiesen wurden — mit Ausnahme der Personen, die einen Selbstmordversuch unternommen haben*

Der Term *leicht verletzte Personen* wird nicht definiert. Im Umkehrschluss der EU-Definitionen kann definiert werden, dass *leicht verletzte Personen* Personen sind, die durch einen Unfall körperlich oder psychisch beeinträchtigt wurden und ambulant bzw. für weniger als 24 Stunden in einem Krankenhaus behandelt werden mussten.

Grundsätzlich ist zu diskutieren, ob bei einer Betrachtung des Schadens leicht verletzte Personen zu berücksichtigen sind, oder ob eine Beschränkung auf schwer verletzte und getötete Personen ausreichend ist. Besonders bei leicht verletzten Personen ist die systematische und zuverlässige statistische Erfassung kompliziert und von vielen Randbedingungen abhängig. Die ERA empfiehlt in ERA-REC-01-2008-SAF (2008) die Berechnung der *gemeinsamen Sicherheitsziele* und der *nationalen Referenzwerte* für *Todesfälle und gewichtete schwere Verletzungen (FWSI)* vorzunehmen. Leicht verletzte Personen werden bei dieser Betrachtung nicht berücksichtigt.

Es wird empfohlen, den Gesamtschaden in Übereinstimmung mit den Vorgaben der ERA ohne Berücksichtigung von Leichtverletzten zu ermitteln. Es kann die Formel zur Berechnung eines Gesamtschadens entsprechend verwendet werden.

$$\text{Opfer} = \text{Tote} + \frac{\text{Schwerverletzte}}{10} \tag{4.22}$$

4.9.5 Explizite und implizite Schadensschätzung

Die Abschätzung des Schädigungsausmaßes der betrachteten Personen ist schwierig. Oft entscheiden Randbedingungen (z.B. körperliche Konstitution, Glück) über den genauen Verletzungsgrad. Es sollte deshalb für die Ermittlung des Schadensausmaßes im Risikographen ein systematischer, ganzheitlicher Ansatz an Stelle einer Einzelfallbetrachtung zur Ermittlung des Schadens gewählt werden.

In vielen herkömmlichen qualitativen Methoden wird der Personenschaden explizit durch Angabe des Schadens abgeschätzt (z.B. DIN EN ISO 13849-1 (2004)). Dies birgt die Gefahr, dass zu hohe Werte angenommen werden, da zum einen Ereignisse mit hohem Schaden mehr in Erinnerung bleiben als Ereignisse mit einem niedrigen Schaden und zum anderen ein Anwender aus Sorge vor einer zu niedrigen Abschätzung zu hohe Werte wählt. Die explizite Schadensschätzung hat den Vorteil, dass der Anwender sieht, mit welchen Werten das Risiko ermittelt wird. Wird eine explizite Schadensschätzung gewählt, muss entschieden werden, ob durch den

Anwender ein Gesamtschaden abgeschätzt wird oder ob eine detaillierte Schadensschätzung für die einzelnen Betroffenheitsklassen erfolgen soll.

Die Möglichkeit der impliziten Schadensschätzung durch den Anwender, d.h. die Abschätzung der Unfallrandbedingungen und die methodeninterne Schadensermittlung, ist abhängig von der Zahl der Einflussgrößen auf den Schaden. In einem Risikographen kann nur eine begrenzte Anzahl von variablen Einflüssen berücksichtigt werden. Es ist ein Vorteil der impliziten Schadensschätzung, dass der Schaden auf Basis weitgehend objektiver Angaben zur betrieblichen Situation ermittelt werden kann.

Es ergeben sich für die Schätzung eines kollektiven Schadens vier grundsätzlich unterschiedliche Vorgehensweisen:

- Es wird ein Gesamtschaden geschätzt (Summe über alle relevanten Schadensklassen).
- Es wird nur der Schaden der höchsten Betroffenheitsklasse geschätzt. Es wird methodenintern unter Annahmen ein Gesamtschaden ermittelt.
- Es wird unabhängig vom Betroffenheitsgrad die Zahl der betroffenen Personen geschätzt. Es wird methodenintern unter Annahmen ein Gesamtschaden ermittelt.
- Es werden die Unfallrandbedingungen beschrieben. Der Konstrukteur hat methodenintern bei der Konstruktion eine Zuordnung der Unfallrandbedingungen zu einem Gesamtschaden vorgenommen.

Es wird eine implizite Schadensschätzung basierend auf betrieblichen Parametern empfohlen. Ein solches Vorgehen wird als zuverlässiger eingeschätzt als die explizite Schadensschätzung, da keine detaillierte Personen- bzw. Personengruppenbetrachtung zu erfolgen hat, sondern weitestgehend auf betriebliche Fakten zurückgegriffen werden kann. Die gemachten Ausagen gelten unabhängig davon, ob bei der Risikoermittlung kollektiver oder individueller Schaden zu berücksichtigen ist.

4.10 Optionen für die Unfallwahrscheinlichkeit

Die Wahrscheinlichkeit, dass sich nach Auftreten einer Gefährdung ein Unfall entwickelt (Unfallwahrscheinlichkeit), wird durch die Reduktionsfaktoren beschrieben. In Gayen u. a. (2002) wird ausgeführt, dass Reduktionsfaktoren externe, vom betrachteten System nicht beeinflussbare Faktoren sind. In Braband (2005) wird der Begriff weiter gefasst. Es wird dort ausgeführt, dass zu den Reduktionsfaktoren gehören:

- physikalische Schutzmaßnahmen, wie technische Diagnose-, Warn-, Kontroll- und Schutzsysteme,
- verfahrenstechnische Schutzmaßnahmen, wie Regeln, Verfahren und Prozesswissen der Bediener,
- sich aus bestimmten Umständen (insbesondere hemmenden betrieblichen Randbedingungen) ergebende Schutzmaßnahmen, wie ungeplante, aber dennoch vorteilhafte Umstände, die einen Unfall verhindern oder abwehren können.

Reduktionsfaktoren gehen in Form von Raten, Häufigkeiten oder Wahrscheinlichkeiten in die Analyse ein.

Bezüglich des maßgeblichen Szenarios für die zu schätzenden Reduktionsfaktoren wird im Allgemeinen bei bisherigen qualitativen Analysen keine Aussage getroffen, d.h. es wird nicht ausdrücklich gefordert, dass beispielsweise die Reduktionsfaktoren auf dem Pfad zum worst-case-Schadensfall liegen oder selbst einen worst-case-Fall (geringste Reduktion, d.h. höchste Unfallwahrscheinlichkeit) darstellen müssen. Grundsätzlich ist zu unterscheiden, ob

- als Reduktionsfaktor die tatsächlich im betrachteten Schadensszenario zu berücksichtigenden Reduktionsfaktoren anzunehmen sind,
- maximale Reduktionsmöglichkeiten anzunehmen sind, d.h. die Unfallwahrscheinlichkeit als niedrig angenommen wird,
- minimale Reduktionsmöglichkeiten anzunehmen sind, d.h. die Unfallwahrscheinlichkeit als hoch angenommen wird,
- mittlere, durchschnittliche (typische) Reduktionsmöglichkeiten angenommen werden.

Wird eine minimale Reduktion, d.h. eine hohe Unfallwahrscheinlichkeit abgeschätzt, so wird das Produkt aus Schaden und Reduktionsfaktor sehr groß. Diese Abschätzung ist zur sicheren Seite, kann aber zu konservative Anforderungen ergeben.

Wird eine maximale Reduktion, d.h. eine niedrige Unfallwahrscheinlichkeit abgeschätzt, so kann nicht beurteilt werden, ob das Risiko richtig abgeschätzt wird. Es besteht die Gefahr, dass das Risiko zu niedrig geschätzt wird.

Wird die zum betrachteten Schadensfall passende Unfallwahrscheinlichkeit abgeschätzt, so wird diese relativ niedrig sein, da Unfälle mit hohem Schaden unter anderem aufgrund der wirksamen Reduktionsmöglichkeiten selten auftreten. Es ist schwierig zu beurteilen, ob das Risiko ausreichend hoch geschätzt wurde.

Das Schätzen von mittleren Reduktionswerten ist nicht einfach. Es ist bekannt, dass der Unfallschaden im Allgemeinen zu hoch geschätzt wird, da extreme Fälle das Erinnerungsvermögen dominieren. Es kann vermutet werden, dass ein ähnlicher Effekt auch beim Abschätzen der Unfallwahrscheinlichkeit eintritt. Zum Einen dominieren vermutlich Ereignisse das Erinnerungsvermögen, in denen ein Unfall gerade nicht verhindert werden konnte (u.a. deshalb, weil die entsprechenden Unfälle zu einem Schaden geführt haben und daher mehr Aufmerksamkeit bekommen haben), und zum anderen werden in dem Bestreben, eine Abschätzung zur sicheren Seite vorzunehmen, tendeziell zu hohe Unfallwahrscheinlichkeiten, d.h. zu wenige Reduktionsmöglichkeiten angenommen. Da dies jedoch zur sicheren Seite geschieht, d.h. das geschätzte Risiko größer ist als das tatsächliche Risiko, sollte dieses Argument nicht gegen das Vorgehen sprechen.

In der Realität setzen sich die meisten Einzelrisiken aus einem relativ geringen Schaden und einer durchschnittlichen, niedrigen Unfallwahrscheinlichkeit zusammen und leisten damit nur einen geringen Beitrag zum Gesamtrisiko. Es gibt typischerweise nur wenige Ereignisse mit hohem Schadensausmaß, die dann im Allgemeinen eine niedrige Unfallwahrscheinlichkeit haben. Dadurch ist der Beitrag dieser Szenarien nicht überproportional groß. Ein Produkt aus der Gefährdungshäufigkeit, einem hohen Schaden und einer typischen, mittleren, tendenziell zu hohen Unfallwahrscheinlichkeit ist deshalb größer als das reale Gesamtrisikos und so eine Abschätzung zur sicheren Seite.

Bei quantitativen Risikoanalysen wird die Wirkung von Reduktionsfaktoren im Allgemeinen als Wahrscheinlichkeit berücksichtigt. Es wird unterschieden, ob ein Reduktionsfaktor einen Unfall verhindert oder nicht. Bisher wird nicht bzw. kaum berücksichtigt, wenn ein Reduktionsfaktor durch sein Wirken einen Unfall nicht verhindert, jedoch das Unfallausmaß reduziert. Dies kann unter Umständen, in Abhängigkeit der Wirkungsweise des Reduktionsfaktors, durch zusätzliche Pfade im Ereignisbaum geschehen. Bei semi-qualitativen Analysen ist ein solches Vorgehen zur Zeit nicht vorgesehen. Hier ist zusätzlicher und umfangreicher, über die Methodenentwicklung hinausgehender Forschungsaufwand zu sehen, der nicht im Rahmen dieser Arbeit erfolgen kann.

4.11 Aussetzungszeit und Gefährdungsdauer

Im Rahmen der Risikoermittlung mittels Risikograph werden Aussetzungszeit und Gefährdungsdauer in einem gemeinsamen Parameter betrachtet. Das zu ermittelnde Risiko wird bei ansonsten gleichbleibenden Parameterklassen umso größer, je größer der Wert für die Summe aus Aussetzungszeit und Gefährdungsdauer wird.

Die Aussetzungszeit E berücksichtigt, wie lange das Betrachtungsobjekt der zu betrachtenden Funktion bzw. der Komponente ausgesetzt ist. Bei der Ermittlung des Wertes ist zu berücksichtigen, wie das Bezugssystem definiert ist. Gegebenenfalls muss eine Abstraktion der realen Situation und deren Abbildung in einem vereinfachten Modell erfolgen. Die Gefährdungsdauer D gibt an, wie lange eine Gefährdung bestehen bleiben kann, bevor es zu einer Aufdeckung kommt. Sowohl die Aussetzungszeit E, als auch die Gefährdungsdauer D können wahlweise detailliert oder als Konstanten in der Methode berücksichtigt werden.

Die Aussetzungszeit kann maximal dem Betrachtungszeitraum entsprechen. Wenn argumentiert werden kann, dass im Allgemeinen der Maximalwert der Aussetzungszeit zu wählen ist oder dass E im Verhältnis zu D deutlich kleiner und daher zu vernachlässigen ist, kann E als Konstante in die Risikographkonstruktion eingehen.

Wenn der Wert für D bei allen betrachteten Gefährdungen gleich ist, bzw. eine Abschätzung für D zur sicheren Seite möglich ist, kann eine Konstante für D angenommen und im Risikograph berücksichtigt werden. Da es unter Umständen nicht möglich ist, einen Maximalwert für D anzugeben, kann es notwendig sein, bei einer detaillierten Abschätzung von D den Risikographen für einen definierten Maximalwert der Gefährdungsdauer auszulegen. Dieser Maximalwert ist dann als Randbedingung für die Anwendung des Risikographen vorzugeben. Wird der Wert für die Gefährdungsdauer größer als der Maximalwert abgeschätzt, kann der Risikograph nicht bzw. nur nach Rücksprache mit den zuständigen Stellen angewandt werden.

4.12 Kalibrierung des Risikographen

Bei der Kalibrierung eines Risikographen wird ein Zusammenhang hergestellt zwischen dem durch Parameterklassen beschriebenen Risiko und einem in der Methode hinterlegten Risikoakzeptanzkriterium. Grundsätzlich sind zwei unterschiedliche Vorgehensweisen zu unterscheiden:

- Berücksichtigung eines tolerierbaren Risikos bei der Risikographkonstruktion,
- Kalibrierung des Risikographen mit einer semi-qualitativen Vorgabe für das Risiko.

Da die Kalibrierung einer Risikoabschätzungsmethode und im Besonderen die Wahl des Risikoakzeptanzkriteriums maßgeblichen Einfluss auf die Konstruktion der Methode haben kann (z.B. auf Risikoart, Ergebnisart, Analyseebene), sollte bereits frühzeitig, sinnvollerweise in Zusammenhang mit der Festlegung der Ergebnisart, eine Aussage zur Methodenkalibrierung bzw. zum Risikoakzeptanzkriterium getroffen werden.

4.12.1 Kalibrierung mittels tolerierbarem Risiko

Das tolerierbare Risiko ist stets nur implizit im Risikographen enthalten und dem Anwender im Allgemeinen nicht bekannt. Es ist eine wesentliche Eingangsgröße bei der Risikographkonstruktion. Um das tolerierbare Risiko korrekt bei der Risikographerstellung berücksichtigen zu können muss

- das tolerierbare Risiko für die gewünschte Analyseebene ermittelt werden,
- ein Zusammenhang zwischen tolerierbarem Risiko und Gefährdung hergestellt werden.

Das tolerierbare Risiko für ein System oder eine Funktion zu ermitteln, ist im Allgemeinen schwierig. Wenn ein neues Produkt analysiert werden soll, welches ein altes Produkt ersetzt, so kann das vom neuen Produkt einzuhaltende, tolerierbare Risiko aus der Analyse des vom bestehenden, zu ersetzenden Produkt ausgehenden Risiko abgeleitet werden. Soll ein neues System bemessen werden, so muss ein tolerierbares Risiko unter Annahmen und Berücksichtigung der Einbindung des Systems in ein Gesamtkonzept abgeleitet werden.

Mit dem Risikographen werden jedoch nicht Systeme analysiert, sondern die aus Fehlfunktionen resultierenden Gefährdungen. Daher muss als Eingangsgröße für die Risikographkonstruktion das tolerierbare Risiko in Abhängigkeit der Gefährdung vorliegen. Hinzu kommt, dass Gefährdungen verschiedener Funktionen unterschiedlicher Systeme möglichst mit einem Risikographen analysiert werden sollen. Es besteht also die Schwierigkeit, wenn das tolerierbare Risiko aus vergleichbaren Systemen ermittelt werden soll, dass es

- unterschiedliche Vergleichssysteme gibt,
- im Allgemeinen für jedes System ein unterschiedliches tolerierbares Risiko gilt,
- im Allgemeinen jede Funktion eines Systems ein unterschiedliches tolerierbares Risiko erlaubt,
- aus jeder Funktion unterschiedlich viele, verschiedene Gefährdungen resultieren können, die ggf. wiederum verschieden große Anteile am Risiko tragen.

In quantitativen Analysen können diese Unterschiede (teilweise) berücksichtigt werden.

Ein Risikograph kann üblicherweise nur unter Berücksichtigung eines Wertes für das tolerierbare Risiko einer Gefährdung konstruiert werden. Ausgangspunkt ist entweder das tolerierbare Risiko für das System oder das tolerierbare Risiko für die Funktion. Das vorgegebene Risiko muss auf die Gefährdungen aufgeteilt werden. Es gibt keine Vorgaben, dass sich die Aufteilung des Risikos auf die Teilsysteme, Teilfunktionen bzw. Gefährdungen am Vergleichsobjekt orientieren muss. Es ist sogar möglich, einzelne Teilsysteme/Teilfunktionen unsicherer auszuführen als im Vergleichsprodukt, solange das Gesamtrisiko eingehalten wird. Dies gilt, solange es in einem System nicht zu einer Mischung aus alten und neuen Teilen kommt, da in

diesem Fall die Möglichkeit besteht, dass das neue Gesamtrisiko größer ist als das bisherige Gesamtrisiko.

Für die Ermittlung des Risikos je Gefährdung können als Lösungsmöglichkeiten diskutiert werden, dass

1. unter der Annahme der Gleichverteilung des Risikos und einer zur sicheren Seite angenommenen Gefährdungszahl ein gefährdungsbezogenes tolerierbares Risiko berechnet wird,

2. für alle Gefährdungen das beim Vergleichssystem kleinste vorkommende gefährdungsbezogene Risiko angenommen wird,

3. die Gefährdungsdefinition so zu erfolgen hat, dass je Funktion nur eine Gefährdung identifiziert werden kann (Gefährdung durch Negierung), so dass das funktionsbezogene und das gefährdungsbezogene tolerierbare Risiko identisch sind,

4. die Risikographmethode so erweitert wird, dass durch Berücksichtigung eines weiteren Parameters unterschiedliche gefährdungsbezogene Risiken berücksichtigt werden können, wobei sichergestellt sein muss, dass das zulässige funktionsbezogene tolerierbare Risiko nicht überschritten wird.

Für das erstgenannte Vorgehen sind Überlegungen zur Zahl der Gefährdungen je Funktion und ggf. zur Zahl der Funktionen je System zu führen. Definitive Aussagen, dass die ermittelten Ergebnisse zur sicheren Seite sind, sind nur bei Berücksichtigung entsprechend großer Sicherheitsmargen möglich. Sind keine neuen Gefährdungen zu erwarten, so führt Vorgehen zwei zu Ergebnissen auf der sicheren Seite. Allerdings besteht die Gefahr, dass zu konservative Ergebnisse ermittelt werden. Die Annahme, dass aus jeder Funktion nur eine Gefährdung entsteht, kann nur für eine sehr hohe Systemebene gerechtfertigt bzw. angenommen werden (siehe z.B. Braband (2005)). Fall vier wird nicht weiter verfolgt, da dies eine wesentliche Erweiterung und Veränderung der Risikographmethode darstellen würde.

Die Ausführungen zeigen, dass selbst bei Vorliegen eines Risikowerts dessen Aufteilung schwierig ist. Hinzu kommt, dass es politisch und technisch schwierig ist, einen allgemein akzeptierten Wert für das tolerierbare Risiko zu erhalten. Die bei der European Railway Agency (ERA) veröffentlichten Statistiken zur Leistung der Eisenbahnunternehmen in Europa zeigen beispielsweise deutliche Unterschiede in den einzelnen Ländern. Es steht nicht zu erwarten, dass es kurzfristig zu einer europäischen Einigung kommt. Die ERA geht nicht davon aus, wie in Cassir (2008a) ausgeführt wird, dass ein Top-Down-Ansatz zur Ableitung von Sicherheitsanforderungen auf niedriger Ebene aus auf hoher Ebene vorliegenden Informationen gangbar ist.

4.12.2 Kalibrierung mittels Benchmarkwerten

Eine zweite Möglichkeit der Risikographkalibrierung besteht darin, dass, basierend auf grundsätzlichen Überlegungen, ein Risiko als Benchmarkwert festgelegt wird. Ein Benchmarkwert stellt einen Zusammenhang zwischen einer Anforderung und einem Szenario her. Aus diesem Einzelfall kann unter Annahmen auf Anforderungen für andere Szenarien geschlossen werden. In Verordnung EG Nr. 352/ (2009) wird semi-qualitativ ein Risiko als Risikoakzeptanzkriterium für technische Systeme (RAC-TS) vorgegeben. Das Szenario wird qualitativ beschrieben.

Für das beschriebene Szenario wird eine einzuhaltende Gefährdungsrate (*THR*) quantitativ vorgegeben. Es wird keine Aussage zu Risikoaversion getroffen.

Es handelt sich um eine generische Festsetzung eines Risikoakzeptanzwertes. In der Vergangenheit wurde bereits einmal eine Analyse durchgeführt, die einen ähnlichen Ansatz verfolgt hat: die Risikoanalyse ESTW Phase 1 (Braband u. a. (2002)). Nach Erstellung einer Systemdefinition und der Gefährdungsidentifikation wurde für jede Gefährdung eine Ursachenanalyse durchgeführt, welche bis auf Subsystem/Komponentenebene herunter gebrochen wurde. Aufgrund der für die technischen Komponenten vorliegenden Daten konnte die Ausfallrate des realisierten Produkts für jede Gefährdung ermittelt werden. Dieses Ergebnis wurde als Sicherheitsziel vorgegeben. In Braband u. a. (2002) heißt es explizit: *Es wurde davon ausgegangen, dass diese Analyse generisch erfolgen kann, das heißt unabhängig von den Betriebsbedingungen sowie von der Größe und Ausstattung eines bestimmten Stellwerks....Da sich diese Annahme während der Analyse als richtig erwiesen hat, war es nicht erforderlich ein Musterstellwerk zu definieren.* Das vorgeschlagene Vorgehen zur Kalibrierung des Risikographen mit RAC-TS entspricht in der grundlegenden Idee dem hier beschriebenen Vorgehen.

Das Vorgehen zur Ableitung von Risikoakzeptanzwerten für weitere Szenarien, ausgehend vom RAC-Benchmarkwert, erfolgt durch eine Betrachtung von Risikoisotonen. Die Risikoakzeptanz kann in einem Diagramm als Risikoisotone (siehe Clemens (1993)), das heißt als Linie gleichen Risikos dargestellt werden. Ausgangspunkt ist die Gleichung zur Ermittlung des Risikos in Risikographen.

$$R = HR \cdot DE \cdot C \cdot F \tag{4.23}$$

Durch das qualitative Szenario werden die Parameter DE_{bm}, C_{bm} und F_{bm} beschrieben, die für eine rechnerische Ermittlung des Risikos einer Gefährdung zu quantifizieren sind. Dem Szenario wird eine zulässige Gefährdungsrate *THR* zugeordnet.

$$R_{bm} = THR \cdot DE_{bm} \cdot C_{bm} \cdot F_{bm} \tag{4.24}$$

In einem Diagramm kann das Produkt aus DE_{bm}, C_{bm} und F_{bm} auf der einen Achse, und der Wert für *THR* auf der anderen Achse abgetragen werden. Es ergibt sich in der Diagrammfläche ein Punkt, der das Benchmarkrisiko der Gefährdung im beschriebenen Szenario beschreibt. Wird der Wert auf der einen Achse um den gleichen Faktor verringert wie der Wert auf der anderen Achse vergrößert wird, so ergeben sich weitere Punkte gleichen Risikos (Bild 4.10).

Im Unterschied zu einer kontinuierlichen Skala in einem Diagramm liegen die Klassengrenzen des Risikographen als diskrete Werte vor. In der Tabelle für die Zuweisung von Sicherheitsanforderungen in DIN EN 61508-1 (2002) kann der Faktor 10 zwischen den Klassengrenzen berechnet werden. Wurde das Risiko durch die Benchmarkparameter festgelegt und sind die Benchmarkparameter gleichzeitig Klassengrenzen, so können unter Annahme des Faktors 10 nach der obigen Beschreibung die Risikowerte für die einzelnen Parameterklassenkombinationen ermittelt werden.

Wenn zwischen den Parameterklassenwerten kein gleichbleibender Faktor liegt oder zwischen den Parameterklassen ein anderer Faktor als zwischen den Ergebnisklassen gewünscht wird, so kann keine direkte Zuordnung der Risikoakzeptanzwerte erfolgen. Eine Möglichkeit, dennoch nachvollziehbare Ergebnisse zu erhalten, besteht darin, an entsprechenden Stellen zu runden.

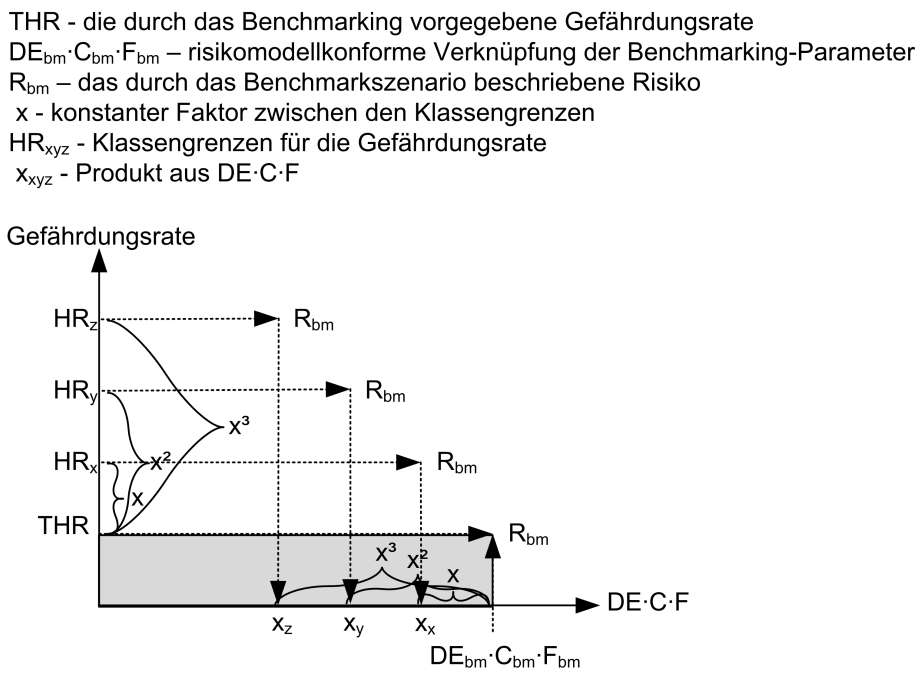

Bild 4.10: Kalibrierung mittels Benchmarkrisiko

Üblich und in der Literatur zu finden ist die Annahme, dass die Risikoakzeptanz einer linearen Verbindung entspricht bzw. als solche angenommen werden kann (z.B. Bepperling (2009)). Diese Annahme kommt aus der Darstellung, bei der ein gleicher Faktor zwischen den Parameterklassenwerten als gleicher Abstand dargestellt wird. Dies ist der Fall, wenn der Abstand zwischen den Klassengrenzen dem Faktor 10 entspricht und eine logarithmische Skalierung der Achsen erfolgt. Unter diesen Bedingungen ergibt sich im Diagramm für die Risikoakzeptanz eine Gerade.

Die Ableitung der Ergebnisklassen unter den in diesem und dem Abschnitt 4.8.5 gemachten Annahmen führt zu einer Ergebnisermittlung wie in Bild 4.11 dargestellt.

Anhand der logarithmischen Darstellung der Risikoakzeptanz kann demonstriert werden, warum die Annahme eines Benchmarkwerts für den ungünstigsten Fall, d.h. für die höchsten Sicherheitsanforderungen, auch bei Berücksichtigung von Risikoaversion zu Ergebnissen auf der sicheren Seite führt[5]. Wird als Ausgangswert für die Wertermittlung der ungünstigste Fall (d.h. hoher Schaden und geringe zulässige Gefährdungsrate) angenommen, so gilt die Risikoakzeptanzkurve auch bei Annahme einer Risikoaversion für hohe Schadenswerte. Würde umgekehrt vom kleinsten Schaden und einer großen zulässigen Gefährdungsrate ausgegangen werden, so würde das Ergebnis nicht zur sicheren Seite ausfallen (siehe Bild 4.12).

4.13 Ergebnisermittlung für latente Gefährdungen

Latente Gefährdungen sind Fehlfunktionen die nur durch das Zusammentreffen des Versagens einer Komponente bzw. eines menschlichen Fehlers mit mindestens einem weiteren Versagen,

[5]Risikoaversion bedeutet, dass für Ereignisse mit hohem Schaden ein im Verhältnis geringeres tolerierbares Risiko gilt als für Ereignisse mit niedrigem Schaden

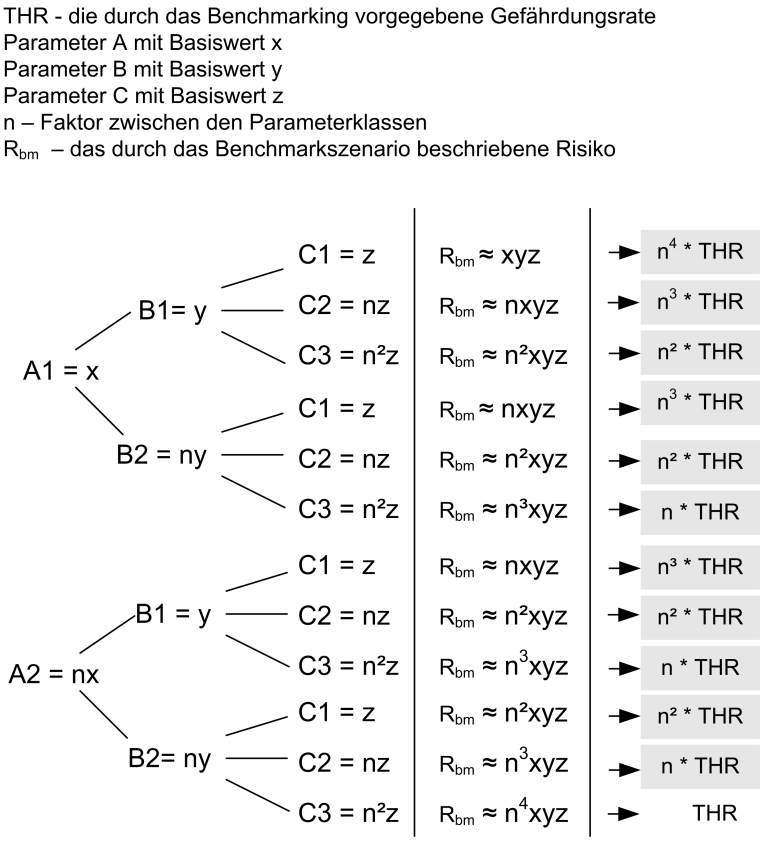

Bild 4.11: Ableitung von Ergebnisklassen bei gleichem Faktor zwischen den Parameterklassen und den Ergebnisklassen

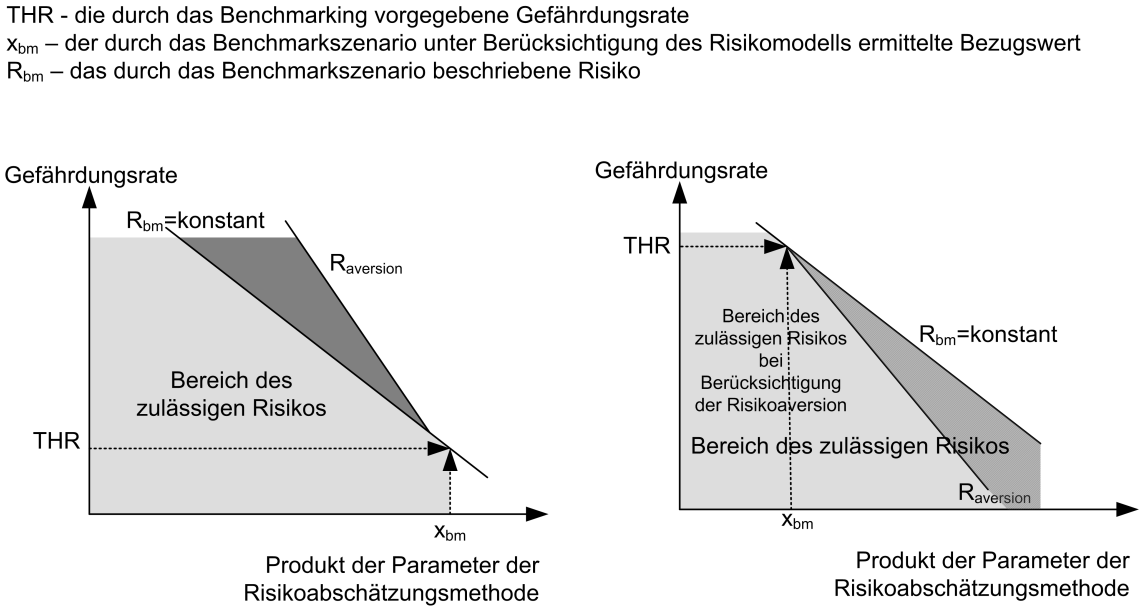

Bild 4.12: Auswirkung der Benchmarkwahl und der Annahmen zum Risiko mit und ohne Berücksichtigung von Risikoaversion

Fehler oder einer besonderen betrieblichen Situation auftreten können. Dies bedeutet, dass das einzelne Versagen zunächst eine Zeit bestehen kann, bevor es zu dem Zusammentreffen mit einem zweiten Ereignis und damit zu einer Fehlfunktion und latenten Gefährdung kommt. Ein Beispiel für ein solches Zusammentreffen ist ein Versagen der punktförmigen Zugbeeinflussung, deren Versagen nur aufgedeckt wird (systeminherente Offenbarungsmechanismen ausgeschlossen), wenn zum (latent vorhandenen) technischen Versagen der Sicherungseinrichtung ein Fehler des Triebfahrzeugführers, d.h. eine fehlende verfahrenskonforme Reaktion hinzukommt.

Wird die latente Gefährdung in einem Ereignisbaum dargestellt, so handelt es sich um eine UND-Verknüpfung. Unter Berücksichtigung von Randbedingungen wie z.B. der Unabhängigkeit der verknüpften Ereignisse, kann die resultierende Wahrscheinlichkeit für die latente Gefährdung aus dem Produkt der Wahrscheinlichkeiten für die Einzelereignisse berechnet werden.

Für die Abschätzung von menschlichen Versagenswahrscheinlichkeiten bzw. -häufigkeiten gibt es Quellen. Zwar kann grundsätzlich diskutiert werden, inwieweit die dort angegebenen Werte sinnvoll und nachvollziehbar sind, jedoch muss in Ermangelung exakterer Werte darauf zurückgegriffen werden.

Die Abschätzung der Versagenswahrscheinlichkeit für technische Systeme ist schwieriger. Ist die Versagensrate bekannt, so kann unter Annahmen zum Wartungsintervall die Wahrscheinlichkeit berechnet werden, dass es in dem relevanten Zeitfenster zu einem Versagen kommt. In günstigen Fällen sind für die relevanten Systeme und die zu berücksichtigenden Fehlfunktionen Sicherheitsanalysen durchgeführt worden, aus denen die benötigten Zahlenwerte entnommen werden können. Es ist im Einzelfall zu prüfen, ob aufgrund der niedrigen anzunehmenden Gefährdungsrate der betrachteten Systeme der gleichzeitige Ausfall zweier technischer Systeme ausgeschlossen werden kann.

4.14 Grenzen für die Ableitung von Sicherheitsanforderungen

Es stellt sich die Frage, ob in einer Risikoabschätzungsmethode für jede Gefährdung eine Sicherheitsanforderung ermittelt werden kann oder ob berücksichtigt werden muss, dass es Gefährdungen gibt, an die höhere Anforderungen als im Risikograph vereinbart, d.h. im Allgemeinen höhere Anforderungen als in DIN EN 61508-1 (2002) angegeben, zu stellen sind. Ein Beispiel ist der Risikograph in DIN EN 61508-5 (2002). Wird in dem dort vorgestellten Risikographen für alle Parameter die maximale Klasse gewählt, so lautet das Ergebnis, dass ein einzelnes E/E/PES, d.h. die Anforderung von 10^{-9} Ausfälle je Betriebsstunde bzw. SIL 4, nicht ausreichend ist.

Zunächst wird das Vorgehen in DIN EN 61508-5 (2002) näher analysiert. Der Risikograph aus DIN EN 61508-5 (2002) ist kein Risikograph zur Anwendung, sondern dient der Illustration des grundsätzlichen Vorgehens. Aufgrund des in DIN EN 61508-1 (2002) beschriebenen Systemmodells dient der Risikograph nicht der Beurteilung des Gesamtsystems, sondern der Bemessung eines sicherheitsbezogenen Systems, welches als zusätzliches System, unabhängig des Systems zum Steuern und Leiten bzw. des EUC zu sehen ist. Damit hat der Risikograph die Aufgabe, das von dem Gesamtsystem ohne sicherheitsbezogene Systeme ausgehende Risiko zu ermitteln und durch Vergleich mit einem tolerierbaren Risiko festzustellen, welche Ausfallrate das sicherheitsbezogene System haben darf, damit das Risiko des Gesamtsystems dem tolerierbaren Risiko entspricht. In diesem Fall muss bei der Konstruktion des Risikograpen

intern eine Berechnung der zulässigen Ausfallraten des sicherheitsbezogenen Systems unter Annahme von Zahlenwerten für alle Parameterklassen des Risikographen erfolgen. Dabei ist der Fall denkbar, dass das System aus EUC und Leit- und Steuerungssystem zu so einem hohen Risiko führt, dass die Anforderungen an ein sicherheitsbezogenes System über SIL 4 bzw. 10^{-9} gefahrbringende Ausfälle je Stunde hinausgehen. Folgerichtig sieht der Beispielrisikograph aus DIN EN 61508-5 (2002) vor, dass in diesem Fall die notwendige Risikoreduktion nicht mit einem sicherheitsbezogenen System erreicht werden kann.

Die Beurteilung der maximal auftretenden Sicherheitsanforderungen erfolgt in Abhängigkeit der Methodenkalibrierung.

Bei der Kalibrierung mittels eines tolerierbaren Risikos müssen für die zum Bemessungsszenario gehörigen Parameterklassen gewählt und quantifiziert werden. Aus diesen Werten und mittels dem Vorgabewert für das tolerierbare Risiko kann eine zulässige Gefährdungsrate berechnet werden, der in einem zweiten Schritt ein Sicherheitsintegritätslevel zugewiesen werden kann. Bei einem solchen Vorgehen ist es möglich, dass Gefährdungsraten berechnet werden, die kleiner sind als der in DIN EN 61508-1 (2002) gegebene Grenzwert von 10^{-9} gefahrbringenden Ausfällen je Stunde. Es muss im Einzelfall entschieden werden, ob die Vorgabe einer so niedrigen Gefährdungsrate sinnvoll ist. Wird für die Zuweisung eines SIL die in DIN EN 61508-1 (2002) gegebene Tabelle herangezogen, so wird eine untere Grenze für SIL 4 festgesetzt zu 10^{-9} Ausfällen je Stunde.

Ist das zur Kalibrierung heranzuziehende Risiko als semi-qualitatives Benchmark formuliert, so ist zu prüfen, inwieweit die mit dem Szenario verbundenen Parameterklassen Maximalwerten entsprechen. Wird das Risikoakzeptanzkriterium RAC-TS betrachtet, so wird ein Ereignis mit katastrophalem Schaden beschrieben. Es kann davon ausgegangen werden, dass dies ein maximales Schadensereignis ist. Es gibt keine Parameterklasse für einen höheren Schaden. Desweiteren wird bei der Beschreibung des Szenario eine Aussage zur Unfallwahrscheinlichkeit getroffen. Es werden keine Reduktionsmöglichkeiten angenommen, so dass der Unfall als unausweichlich anzunehmen ist. Dies entspricht einer maximalen Unfallwahrscheinlichkeit. Da es für beide Parameter keine ungünstigeren Parameterklassen gibt und unter der Annahme, dass keine weiteren Einflüsse zu betrachten sind, beschreibt das Kriterium das ungünstigste Szenario und stellt einen Grenzwert dar. Schärfere Anforderungen bzw. der Hinweis, dass eine Realisierung nicht möglich ist, können nicht Ergebnis der Analyse sein, da es keine entsprechenden Parameterklassen gibt. Sind im Rahmen der Kalibrierung mit dem Benchmarkszenario für weitere Parameter Annahmen zu treffen, die nicht dem ungünstigsten Fall entsprechen, so entspricht die ermittelte Gefährdungsrate nicht den höchsten Anforderungen. Es kann im Rahmen einer Analyse eine schärfere Anforderung, d.h. eine niedrigere Gefährdungsrate gefordert werden.

Kapitel 5

Konstruktion eines Risikographen

5.1 Grundlagen

In diesem Kapitel werden die Arbeitsschritte zur Risikographerstellung diskutiert. Parallel dazu wird ein Beispielrisikograph konstruiert. Der zu erstellende Risikograph soll als Alternative zu dem in VDV 332 (2008) *Sicherheitsintegritätsanforderungen für Bahnsignalanlagen bei Nichtbundeseigenen Eisenbahnen (NE)* vorgestellten Risikographen konstruiert werden. Daraus ergeben sich die einzuhaltenden Randbedingungen:

- Es sind die für das Eisenbahnwesen relevanten Normen zu berücksichtigen.
- Die Anwendung erfolgt für die Funktionen von Bahnsignalanlagen.
- Es sind typische betriebliche Randbedingungen von Nichtbundeseigenen Bahnen zu berücksichtigen.

Die Konstruktionsschritte folgen dem im vorhergehenden Kapitel vorgestellten Ansatz und orientieren sich am in DIN EN 50126 (2000) definierten Lebenszyklusprozess.

5.2 Anwendungsbereich

In Abschnitt 4.2 wurden drei mögliche Festlegungen für den Anwendungsbereich diskutiert:

- generische Risikographen,
- generisch-anwendungsbezogene Risikographen und
- spezifische Risikographen.

Der im Rahmen der Beispielkonstruktion zu erstellende Risikograph ist ein generisch-anwendungsbezogener Risikograph: Er soll angewendet werden auf die aus unterschiedlichen Funktionen von Bahnsignalanlagen erwachsenden Gefährdungen.

5.3 Ergebnisart

In Abschnitt 4.3 wurden drei mögliche Ergebnisarten diskutiert:

- Angabe einer notwendigen Risikoreduktion,
- Angabe eines einzuhaltenden Safety Integrity Levels,
- Angabe einer einzuhaltenden Gefährdungsrate.

Es wird die Gefährdungsrate als geeignete Form der Vorgabe von Sicherheitsanforderungen gewählt. Für technisch zu realisierende Funktionen kann anhand z.B. der in DIN EN 61508-1 (2002) gegebenen Tabellen basierend auf den ermittelten Gefährdungsraten ein Safety Integrity Level abgeleitet werden.

5.4 Risikoakzeptanzkriterium und Kalibrierung

In Abschnitt 4.12 werden zwei grundsätzlich unterschiedliche Arten der Methodenkalibrierung unterschieden:

- Kalibrierung mittels tolerierbarem Risiko,
- Kalibrierung mittels Benchmarkwert.

Zur Kalibrierung des Risikographen wird das in Verordnung EG Nr. 352/ (2009) vorgeschlagene Risikoakzeptanzkriterium für technische Systeme[1] angewendet. Die anzuwendende Passage aus Verordnung EG Nr. 352/ (2009) ist folgende:

Wenn sich aus Ausfällen technischer Systeme Gefährdungen ergeben, die nicht von den anerkannten Regeln der Technik oder der Verwendung eines Referenzsystems abgedeckt werden, gilt das folgende Risikoakzeptanzkriterium für die Planung technischer Systeme:

Bei technischen Systemen, bei denen die Annahme gerechtfertigt ist, dass ein funktionaler Ausfall katastrophale Folgen hätte, muss das damit verbundene Risiko nicht weiter eingedämmt werden, wenn die Ausfallrate pro Betriebsstunde kleiner oder gleich 10^{-9} *ist.*

Bezüglich der Aussage gibt es zwei verschiedene Interpretationen:

- Der angegebene Zahlenwert gilt für die Erfüllung der Funktion während einer Stunde. Es ist ein Gesamt-Zielwert. Wird die Funktion von mehreren (gleichen) technischen Komponenten erbracht, so ist der von den einzelnen technischen Komponenten einzuhaltende Zahlenwert u.U. deutlich niedriger (Bild 5.1, links).
- Der angegebene Zahlenwert ist für eine Komponente und eine Stunde gültig ist. In diesem Fall kann der Zahlenwert direkt als Vorgabewert für die Herstellung der entsprechenden Komponente genutzt werden (Bild 5.1, rechts).

Drei Argumente sollen an dieser Stelle zeigen, dass die zweite Interpretation sinnvoll und zukunftsweisend ist.

Würde die erste Interpretation verfolgt werden, so hätte die Infrastruktur der Strecke wesentlichen Einfluss auf die zulässige Gefährdungsrate einer Komponente. Sowohl national als auch international könnten unterschiedliche Zahlenwerte abgeleitet werden. Eine gegenseitige Anerkennung, wie sie in Verordnung EG Nr. 352/ (2009) bei Einhaltung von RAC-TS zugesichert wird, wäre nicht nachvollziehbar.

[1] Der Begriff System kann unterschiedlich interpretiert werden. Im Folgenden wird bei eigenen Texten im Allgemeinen der Begriff Komponente als Bezeichnung für eine kleinere, in sich abgegrenzte, technisch realisierte Betrachtungseinheit verwendet.

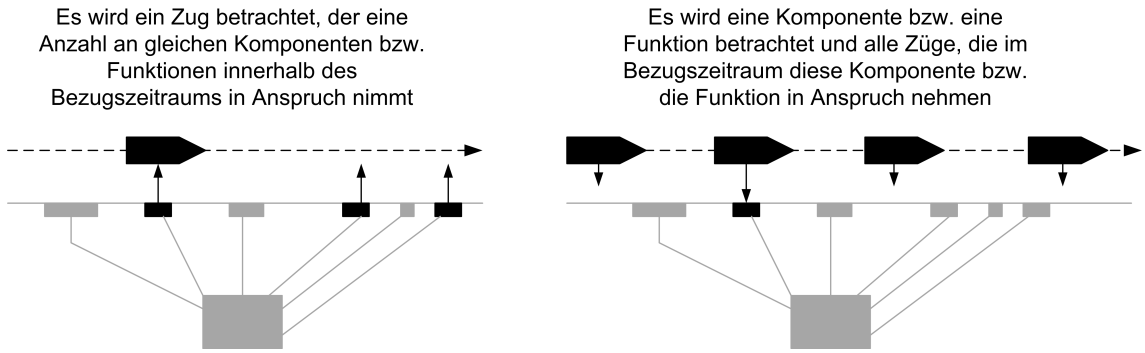

Bild 5.1: Möglichkeiten der Interpretation von RAC-TS

Eine Ableitung der Gefährdungsrate entsprechend der zweiten Interpretation hat zur Folge, dass für unterschiedliche Strecken in Abhängigkeit der vorhandenen Infrastruktur ein unterschiedliches Risiko berechnet werden kann. Dies entspricht der Realität, in der aufgrund der unterschiedlichen Streckenausstattung und des unterschiedlichen Betriebsprogramms bereits unterschiedliche streckenabhängige Risiken bestehen. Es ist nicht zu erwarten, dass zukünftig alle Strecken das gleiche Risiko tragen werden. Risikoaussagen zu einzelnen Strecken sind im Allgemeinen abzulehnen. Aussagekräftig ist nur eine netzweite Betrachtung.

Die Aussage gilt für *technische Systeme*, die einen *funktionalen Ausfall* haben, nicht für Funktionen, die versagen bzw. zu einer Fehlfunktion führen.

5.5 Systemmodell

In Abschnitt 4.4 wird ein für das Eisenbahnwesen allgemeingültiges Systemmodell abgeleitet. Das der Beispielrisikographerstellung zu Grunde zu legende Systemmodell ist ein Spezialfall des allgemeinen Systemmodells. Das Systemmodell für die Risikographanwendung wird ausgehend vom Betrachtungsobjekt entwickelt.

Die in Abschnitt 4.4 gegebene Begründung für den Zug als Betrachtungsobjekt ist weiterhin gültig.

Auf den Zug wirken Funktionen, die den Zug fahren, leiten, steuern und sichern. In VDV 332 (2008) wird ausgeführt, dass der Risikograph für Basisfunktionen des Fahrbetriebs gelten soll. Die zugehörige Tabelle zeigt, dass darunter Funktionen verstanden werden, die die Sicherheit des Zuges gewährleisten. Für das Systemmodell werden sichernde Funktionen als maßgeblich festgelegt. Es kann diskutiert werden, ob die in VDV 332 (2008) genannten Funktionen auch dem Leiten des Zuges dienen. Es wird davon ausgegangen, dass ggf. zu berücksichtigende, leitende Funktionen auch eine Sicherheitsaufgabe haben, und daher in den sichernden Funktionen mit berücksichtigt sind.

Das Dokument VDV 332 (2008) gilt unter den Randbedingungen Nichtbundeseigener Eisenbahnen. Es wird unterschieden nach Bahnen mit Reisezugverkehr und Bahnen mit Güterzugverkehr. Inwieweit die Analyse der beiden Szenarien mit dem gleichen Risikographen möglich ist, ist zweifelhaft, da von unterschiedlichen Risikoakzeptanzkriterien und unterschiedlicher Schadensbetrachtung auszugehen ist. Für die Risikographkonstruktion wird Reisezugverkehr als maßgeblich angenommen.

Es heißt in VDV 332 (2008), dass die *bei NE-Bahnen bestehenden Verhältnisse mit Ge-*

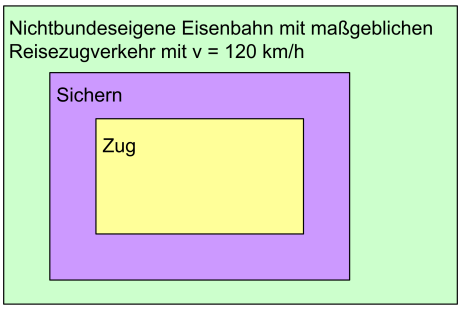

Bild 5.2: Systemmodell als Grundlage für Risikographerstellung

schwindigkeiten bis zu 100 km/h zu Grunde gelegt werden. Da es sich bei den meisten Nichtbundeseigenen Eisenbahnen um Nebenbahnen handelt, stimmt die angenommene Geschwindigkeit mit der in EBO (1967) festgelegten Maximalgeschwindigkeit für Nebenbahnen überein. Es gibt auch Nichtbundeseigene Eisenbahnen, die keine Nebenbahnen sind (z.B. Rheinuferbahn, Vorgebirgsbahn). Im Rahmen der Risikographkonstruktion wird davon ausgegangen, dass durch Verbesserungen und steigende Anforderungen der Reisenden an die Verkehrsverbindungen eine Geschwindigkeitserhöhung anzustreben sein wird. Die Risikographkonstruktion wird daher von einer maximalen Geschwindigkeit von 120 km/h ausgehen. Die Umgebung wird beschrieben als Nichtbundeseigene Eisenbahn mit maßgeblichem Reisezugverkehr mit Geschwindigkeiten bis zu 120 km/h.

Das resultierende Systemmodell ist in Bild 5.2 dargestellt.

Es wird für die weitere Betrachtung davon ausgegangen, dass sich die zu betrachtenden Strecken der Nichtbundeseigenen Bahnen an den Streckenstandards R 80 und R 120 der Deutschen Bahn orientieren. Die Streckenstandards R 120 und R 80 werden in Richtlinie 413 (2002) definiert. Im Anhang dieser Arbeit, Abschnitt 8, werden die wesentlichen Informationen zu den beiden relevanten Streckenstandards zur Verfügung gestellt.

5.6 Analyseebene und Definition der Funktionen

Im Abschnitt 4.5 wurden die Vor- und Nachteile einer niedrigen bzw. einer hohen Analyseebene diskutiert. Im Rahmen der Risikographkonstruktion können die dort gemachten Angaben nur bedingt berücksichtigt werden, da der Risikograph in Anlehnung an VDV 332 (2008) zu konstruieren ist und in diesem Rahmen bereits eine Analyseebene durch Nennung der zu betrachtenden Funktionen bzw. Schutzfunktionen festgelegt wurde. Es ist zu prüfen, ob die Analyseebene durch VDV 332 (2008) ausreichend definiert ist und die genannten Funktionen bzw. Schutzfunktionen den in der Arbeit gestellten Anforderungen genügen. Es ist abzugleichen, ob die gewählte Analyseebene die Anwendung von RAC-TS zulässt.

In Abschnitt 4.6 wird ausgeführt, dass Funktionen entsprechend DIN EN 50129 (2003) als *Art von Aktion oder Tätigkeit, durch die ein Produkt seinen beabsichtigten Zweck erfüllt* definiert werden können. Aufgrund der fehlenden bzw. widersprüchlich oder nicht eindeutig vorliegenden Definitionen für Sicherheitsfunktion, wird Sicherheitsfunktion wie folgt definiert: *Alle Funktionen, an die im Rahmen des Sicherheitsnachweises Anforderungen gestellt werden, bzw. für die im Sicherheitsnachweis Annahmen getroffen werden, werden als Sicherheitsfunktionen bezeichnet.* Es wurde deutlich gemacht, dass im Rahmen der Risikoabschätzung zunächst die Funktionen analysiert werden und im Ergebnis der Abschätzung Funktionen ggf.

als Sicherheitsfunktionen bezeichnet werden können.

In VDV 332 (2008) wird keine generische Definition der Analyseebene und keine komplette Liste der mit dem Risikographen analysierbaren Funktionen gegeben, sondern es werden beispielhaft Schutzfunktionen betrachtet. Es wird nicht definiert, was unter einer Schutzfunktion zu verstehen ist. Es heißt lediglich: *...stellt projektunabhängige Sicherheitsintegritätsstufen für Schutzfunktionen auf, die in generischen Anwendungen verwendet werden können. Die Funktionen von derartigen generischen Anwendungen bzw. sicherungstechnischen Teilsystemen (z.B. EOW) sind in einschlägigen Regeln der Technik (z.B. VDVSchriften) definiert und mit ihren Rahmenbedingungen langjährig bekannt.* Aus den Beispielen kann abgeleitet werden, dass die Schutzeinrichtungen von Komponenten betrachtet werden. Die Auswirkungen des Versagens der Schutzeinrichtungen werden analysiert. Dieses Vorgehen ist nicht stringent, da für Komponenten, die ausschließlich sichernde Aufgaben haben, betrachtete Schutzeinrichtung und Komponente gleich sind.

Das Vorgehen in VDV 332 (2008) ist nicht eindeutig und nachvollziehbar genug, um Basis für die Erstellung und Anwendung eines Risikographen zu sein. Für den zu erstellenden Risikographen wird die Trennung von Komponente und Schutzeinrichtung aufgegeben. Es werden die Fehlfunktionen der von den Komponenten auszuführenden Funktionen analysiert.

Um die durch VDV 332 (2008) vorliegende Basis von Komponenten und Funktionen zu erweitern, werden weitere Beschreibungen des Systems Eisenbahn betrachtet. Im Folgenden werden die in Abschnitt 4.6 vorgestellten Systembeschreibungen auf ihre Eignung als Grundlage für die Risikographkonstruktion diskutiert.

- prEN 0015380-4: Die gegebene Liste von Funktionen ist sehr umfangreich und deckt im Wesentlichen Bereiche ab, die nicht für den Risikographen relevant sind, da es sich um Schienenfahrzeugfunktionen handelt. In Bepperling (2009) wird die Liste zum Teil weiterentwickelt, aber auch der dort vereinbarte Scope ist nicht mit dem Ansatz in VDV 332 (2008) vereinbar.

- Generic Hazard List Methodolgy (UIC (2007)): Der grundsätzliche Ansatz des Vorgehens, sich an der realisierten Technik zu orientieren, stimmt mit der Grundidee des VDV-Risikographen überein. Es werden nicht explizit Funktionen betrachtet. Allerdings sind im Sinne der Risikographerstellung nicht die identifizierten Gefährdungen relevant, sondern die zugeordneten Versagen. Diese Versagen können, als Gefährdungen interpretiert, Grundlage für die Analyse mit dem Risikographen sein.

- Projekt ROSA: In Klinge u. a. (2008) werden ausschließlich Gefährdungen genannt, keine Funktionen. Es ist daher im engeren Sinn keine funktionale Systembeschreibung. Gefährdungen werden ausgehend von Systemfehlern ermittelt. Die logische Struktur der Gefährdungsableitung ist nicht nachvollziehbar. Die in Klinge u. a. (2008) gegebene Zusammenstellung der Starting Point Hazards zeigt, dass diese nicht geeignet sind für die Anwendung im Risikographen.

- Ansatz nach Bosse u. Gayen (2008): Der vorgestellte Ansatz ist für die Anwendung im Rahmen der Risikographerstellung bedingt geeignet. Die realisierungsunabhängige Beschreibung ist für die Risikographanwendung nicht notwendig bzw. nicht gewünscht, weil von einer realisierungsnahen Anwendung des Risikographen ausgegangen wird. Allerdings können u.U. den Funktionen Komponenten zugeordnet werden. In diesem Fall kann die funktionale Beschreibung als Grundlage für den Risikographen dienen. Da

UIC (2007)	VDV 332 (2008)
Weiche (*point*)	Weiche
Gleissperre (*derailer*)	
abschließbare Elemente (*lockable devices*)	
Bahnübergang (*level crossing*)	
Gleisfreimeldung (*TVP section*)	Gleisfreimeldung
Streckenblock (*line block*)	
Bahnhofsblock (*interlocking communication device*)	
Zugbeeinflussung (*ATP device*)	Zugbeeinflussung
Signal (*signal*)	Signal
	Führerstandssignalisierung

Tabelle 5.1: Vergleich der Komponenten aus UIC (2007) und VDV 332 (2008)

jedoch die vorliegende Literatur zu dem Verfahren nicht ausreichend ist, kann dieser Ansatz nicht weiter verfolgt werden.

- Ansatz nach Eickmann u. a. (2008): Vorausgesetzt, dass die funktionale Beschreibung des Systems Eisenbahnverkehr bis zu einer ausreichend niedrigen Systemebene fortgesetzt wird, ist die Nutzung der erstellten Funtionsübersicht für den Risikographen möglich. Der Vorteil des Vorgehens im Unterschied zum Ansatz nach Bosse u. Gayen (2008) ist die anwendungsnahe Funktionsableitung, die der Intention des Risikographen entspricht. Die in Eickmann u. a. (2008) gemachten Ausführungen reichen jedoch weder zu einer abschließenden Beurteilung, noch für die Anwendung im Rahmen des Risikographen aus.

Für die Beispielkonstruktion des Risikographen werden die in VDV 332 (2008) betrachteten Komponenten mit den in UIC (2007) identifizierten Komponenten verglichen (Tabelle 5.1) und der weiteren Arbeit zu Grunde gelegt.

In Anlehnung an die Argumentation in UIC (2007) wird die Ebene zur Anwendung mit dem Risikographen definiert als Ebene, die alle diejenigen physischen Komponenten enthält, die entweder in Zusammenarbeit mit dem Stellwerk oder als selbständige Komponenten die Sicherheit eines Zuges durch ihr Wirken direkt herstellen. Werden noch nicht in UIC (2007) oder VDV 332 (2008) berücksichtigte Komponenten identifiziert (z.B. Element Balise), so können sie mit dem Risikographen analysiert werden, wenn sie der gegebenen Definition genügen. Um den Anforderungen der Norm (z.B. DIN EN 50129 (2003)) genüge zu tun und die Vollständigkeit der identifizierten Funktionen begründen zu können, ist ein systematischer Zusammenhang zwischen Komponenten und Funktionen herzustellen.

Es ist zu prüfen, ob bei dem in diesem Abschnitt vorgeschlagenen Vorgehen die Kalibrierung mittels RAC-TS möglich ist, d.h. es ist zu prüfen, ob RAC-TS für die beschriebene Analyseebene gültig ist. RAC-TS gilt für technische Systeme. Ein technisches System wird in Verordnung EG Nr. 352/ (2009) definiert als *das Bauteil oder die Baugruppe, einschließlich Planung, Realisierung und Begleitdokumentation; die Entwicklung eines technischen Systems beginnt mit der Festlegung der Anforderungen an das System und endet mit seiner Zulas-*

sung; auch wenn dabei die relevanten Schnittstellen zum menschlichen Verhalten berücksichtigt werden, sind das Personal und dessen Handlungen nicht Bestandteil eines technischen Systems; der Wartungsprozess wird in den Wartungshandbüchern beschrieben, ist aber selbst nicht Bestandteil des technischen Systems. Die Komponenten, die als Basis für die Analyseebene definiert wurden, widersprechen nicht der Definition. RAC-TS gilt für einen *funktionalen Ausfall.* In der Beispielanwendung kann jeder Komponente der Analyseebene mindestens eine Funktion zugeordnet werden. Darauf basierend können die Funktionsversagen abgeleitet werden. Es heißt weiter in Verordnung EG Nr. 352/ (2009), dass das durch RAC-TS beschriebene Funktionsversagen *unmittelbare katastrophale Folgen* haben muss. Eine Betrachtung der Komponenten auf der gewählten Analyseebene macht deutlich, dass es Fehlfunktionen gibt, die direkt zu einem Unfallereignis mit katastrophalen Folgen führen können. Es kann geschlussfolgert werden, dass bei Anwendung der gewählten Analyseebene eine Kalibrierung mit RAC-TS möglich ist.

5.7 Gefährdungen

5.7.1 Grundlagen

Aus den Funktionen der identifizierten Komponenten sind die Gefährdungen abzuleiten. In Abschnitt 4.7 wird definiert, dass

- eine Gefährdung eine Fehlfunktion zur unsicheren Seite mit einem Potential von analyserelevantem Schaden ist,
- Gefährdungen als Zustand zu definieren sind,
- zwischen latenten und direkten Gefährdungen unterschieden werden kann,
- nicht davon ausgegangen wird, dass gefährliche Zustände durch systeminterne Prozesse automatisch und ohne Aufdeckung in sichere Zustände zurückgeführt werden,
- die Gefährdungsableitung durch Negierung der Funktion oder durch detaillierte Ausfallbetrachtung erfolgen kann.

In UIC (2007) erfolgt eine detaillierte Versagensbetrachtung der Funktion, aus der durch Kombination mit möglichen Unfalltypen die Gefährdungen abgeleitet werden. Je betrachtetem Element werden mehrere Versagen und daraus resultierend mehrere Gefährdungen abgeleitet. In Abschnitt 4.7 wird ausgeführt, dass die Ermittlung der Sicherheitsanforderungen an eine Funktion schwieriger ist, wenn je Funktion mehrere Gefährdungen identifiziert und analysiert werden. Daher wird vorgeschlagen, dass nicht die Versagensarten aus UIC (2007) als Fehlfunktionen, d.h. Gefährdungen übernommen werden, sondern dass die Gefährdungen durch Negierung der Funktion abgeleitet werden.

5.7.2 Latente und direkte Gefährdungen

Es können sowohl latente als auch direkte Gefährdungen mit dem Risikographen analysiert werden. Bei latenten Gefährdungen liegt eine UND-Verknüpfung von mindestens zwei Ereignissen vor.

Sowohl eine latente, als auch eine direkte Gefährdung können nur zu einem Unfallereignis führen, wenn die Funktion durch einen Zug in Anspruch genommen wird. Das Ereignis *Zug*

kommt bzw. *Zug nimmt das Element in Anspruch* wird als notwendig für das Eintreten einer Fehlfunktion erachtet und ist bei der Definition latenter Gefährdungen nicht zu berücksichtigen (siehe Abschnitt 5.11).

Gefährdungen, die auf das Zusammentreffen zweier unabhängiger technischer Versagen beruhen, können nicht mit dem zu konstruierenden Risikographen analysiert werden. Aufgrund der im Eisenbahnwesen üblichen, äußerst niedrigen technischen Versagensraten ist das Zusammentreffen zweier unabhängiger technischer Versagen sehr unwahrscheinlich und dürfte ausserhalb der mit einer semi-qualitativen Methode erzielbaren Genauigkeit liegen. Es ist möglich, einen Teil der Analyse solcher latenter Gefährdungen mit dem Risikographen vorzunehmen. In diesem Fall kann zunächst die Komponente mit ihrer Funktion im Risikographen untersucht werden. In einem zweiten Schritt kann mit dem ermittelten Wert und dem für die zweite Komponente anzunehmenden bzw. bekannten Wert ein resultierendes Ergebnis berechnet werden.

Das Zusammentreffen von technischem Versagen und menschlichem Fehler muss berücksichtigt werden, da das Zusammenspiel von Technik und Mensch zur Funktionserbringung bzw. Funktionsüberwachung im Eisenbahnwesen häufig vorkommt. Die Fehlerrate eines Menschen ist im Allgemeinen deutlich höher als die Versagensrate von Technik. Daher erscheint eine solche Betrachtung im Rahmen einer semi-qualitativen Methode sinnvoll. Es ist bei der Risikoanalyse zu unterscheiden, ob der Mensch in einer latenten Gefährdung berücksichtigt wird (wenn die Handlung Bedingung für das Eintreten der Fehlfunktion ist), oder ob der Mensch im Rahmen der Unfallwahrscheinlichkeit zu berücksichtigen ist (wenn seine Handlung nach Eintreten der Fehlfunktion zur Unfallvermeidung beiträgt).

Das Zusammentreffen von zwei menschlichen Fehlern zum Erzeugen einer Fehlfunktion ist für den Beispielrisikographen nicht relevant, da aufgrund der Kalibrierung mittels RAC-TS eine Anwendung nur auf die von technischen Komponenten ausgeführten Funktionen möglich ist.

Für den zu erstellenden Risikographen werden die folgenden Bedingungen festgesetzt:

- Es werden nur solche latenten Gefährdungen betrachtet, die durch das Zusammentreffen von genau zwei Ereignissen entstehen.
- Es wird davon ausgegangen, dass es sich bei den Ereignissen um ein technisches Versagen und einen menschlichen Fehler handelt.

5.8 Risiko im Risikographen

5.8.1 Qualitatives Risikomodell

Das qualitative Risikomodell ist eine Spezifizierung des Systemmodells unter Berücksichtigung äußerer Randbedingungen. Es werden zunächst die sich aus dem vorhergehenden Abschnitten ergebenden, relevanten Randbedingungen zusammengestellt.

Durch die Festlegung der Ergebnisart „Gefährdungsrate“ ergeben sich keine Einflüsse auf das Risikomodell. Durch Festlegung des Risikoakzeptanzkriteriums RAC-TS ergibt sich eine Beschränkung der Risikographanwendung auf technische Systeme. Es erfolgt keine Aussage bezüglich der Risikoart oder zu den Parametern der Risikobeschreibung. Es wurde spezifiziert, dass der Risikograph anzuwenden ist auf der Ebene der Funktionen, die alle physischen Komponenten enthält, die entweder in Zusammenarbeit mit dem Stellwerk oder als selbstän-

dige Komponenten die Sicherheit eines Zuges durch ihr Wirken direkt herstellen. Des Weiteren hat das Systemmodell Aussagen zur anzunehmenden betrieblichen Umgebung getroffen.

Basierend auf dem Systemmodell ist das Risiko unter Berücksichtigung der Randbedingungen Nichtbundeseigener Eisenbahnen zu ermitteln für einen Reisezug, der durch eine Fehlfunktion einer sichernden Funktion zu schaden kommt. Für die Ermittlung des Risikos muss eine Aussage getroffen werden zur Unfallhäufigkeit und zum Schaden.

Es stehen verschiedene Möglichkeiten der Schadensermittlung zur Verfügung. Aufgrund der Aussagen in den relevanten Gesetzen, Normen und der Literatur erscheint es zielführend, wenn Personenschaden betrachtet wird. Der Schutz der Personen erfolgt implizit über einen Schutz des Zuges. Es kann davon ausgegangen werden, dass eine Begrenzung des Personenschadens auch zu einer Begrenzung von Sach- und Umweltschaden führt.

Es kann unterschieden werden nach der Art der zu Schaden gekommenen Personen. In Übereinstimmung mit bisherigen Analysen im Eisenbahnwesen kann eine Beschränkung auf Reisende erfolgen, da davon ausgegangen wird, dass durch einen Schutz der Reisenden auch Dritte und Mitarbeiter geschützt sind. Es kann das Risiko wahlweise für eine Einzelperson oder das Kollektiv aller Passagiere im betroffenen Zug ermittelt werden. Es wird ein kollektives Risiko ermittelt, da dieses mit weniger Annahmen und Randbedingungen ermittelt werden kann.

Das zu betrachtende qualitative Risikomodell wird wie folgt formuliert: Es wird unter den Randbedingungen aus dem Betrieb Nichtbundeseigener Eisenbahnen das kollektive Risiko der Reisenden in einem Zug aufgrund der Fehlfunktion sichernder technischer Funktionen ermittelt.

Die Unfallrate wird ermittelt durch Betrachtung der Gefährdungsrate und der Unfallwahrscheinlichkeit. Da es nur zu einem Unfall kommen kann, wenn eine Funktion angefordert wird, ist die Aussetzungszeit, d.h. die Zeit, die der Zug bzw. die betrachtete Personengruppe der Funktion ausgesetzt ist, zu berücksichtigen. Je länger eine Gefährdung besteht, desto wahrscheinlicher wird es, dass es zu einem Unfall kommt.

5.8.2 Risikoformel

Um die qualitative Beschreibung in eine quantitative Formel zu überführen, kann entweder eine Risikoformel unabhängig abgeleitet oder eine bereits existierende Formel spezifiziert werden.

Das kollektive, zugbezogene Risiko *CRF* kann, wie in Abschnitt 4.8.3 hergeleitet, für die Randbedingungen einer qualitativen Risikoabschätzungsmethode ermittelt werden zu

$$CRF = (HR \cdot D + HR \cdot E) \cdot (C \cdot F) \tag{5.1}$$

$$CRF = HR \cdot (D + E) \cdot (C \cdot F) \tag{5.2}$$

Für die Anwendung im Risikographen wird vereinfacht

$$R = HR \cdot DE \cdot C \cdot F \tag{5.3}$$

Es wurde bereits ausgeführt, dass die im Rahmen von RAC-TS gegebene Ausfallrate komponentenbezogen zu interpretieren ist. Um diese Interpretation mit den Anforderungen der Formel zur Ermittlung des kollektiven Risikos in Übereinstimmung zu bringen, muss der tatsächliche Bahnbetrieb abstrahiert werden (Bild 5.3).

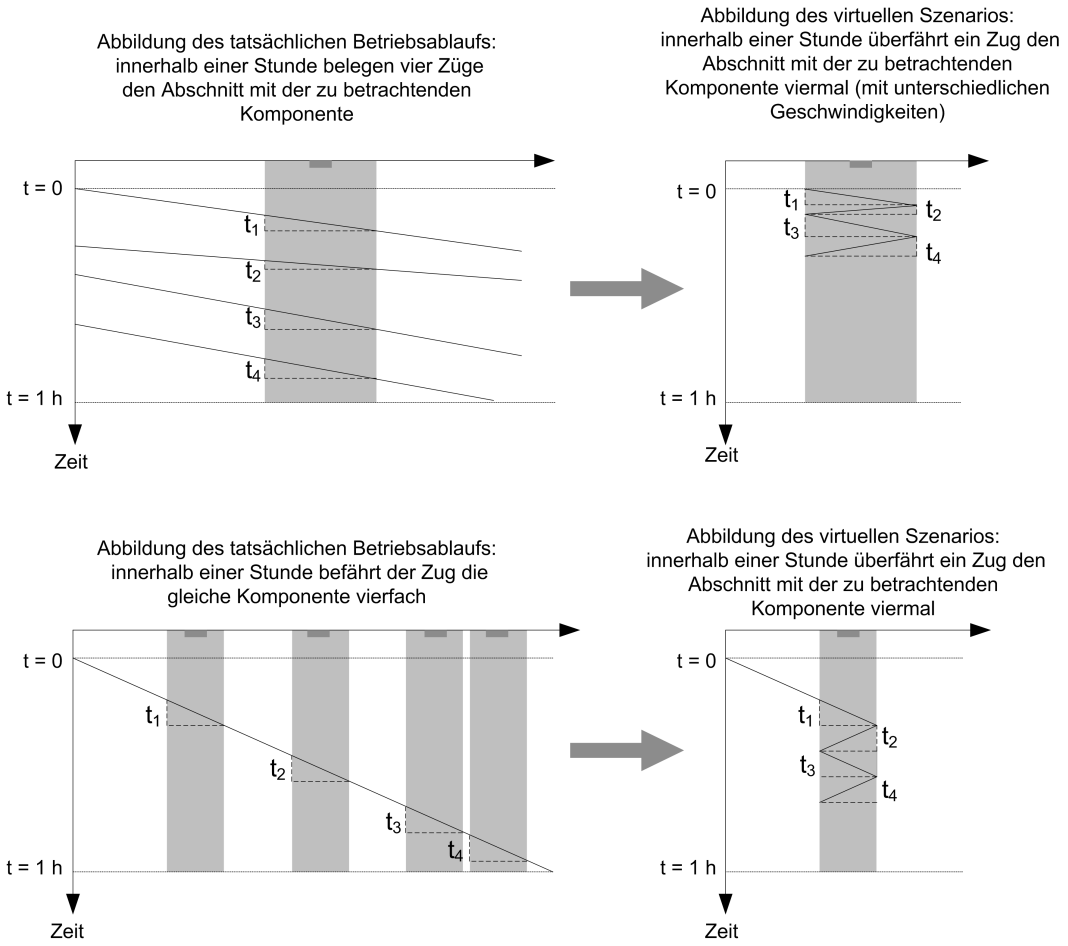

Bild 5.3: Von der Realität zum virtuellen Szenario

In der Realität wird eine Komponente im Lauf einer Stunde von mehreren Zügen befahren. Im Allgemeinen ist jede Person im Zug der Komponente nur kurz ausgesetzt. Es befahren innerhalb einer Stunde mehrere Züge die Komponente. Es wird abstrahiert, dass ein Zug betrachtet wird, der die zu analysierende Komponente so oft innerhalb einer Betriebsstunde befährt, wie die Gesamtheit aller Züge laut Betriebsprogramm dies tun würde. Es wird davon ausgegangen, dass der Zug zwischen zwei Stationen pendelt. Er fährt mit der laut Betriebsprogramm bzw. Streckeninformation vorgegebenen Geschwindigkeit. Alle Abschätzungen für die Parameter zur Berechnung des kollektiven Risikos beziehen sich auf den Zug sowie die Personen im Zug des abstrahierten Szenarios.

Ein alternatives Vorgehen betrachtet einen Zug über den Bezugszeitraum, d.h. über eine Stunde und berücksichtigt, wie oft der Zug die gleiche Komponente überfahren hat. Auch dieses Szenario kann entsprechend obiger Annahme abstrahiert werden. Da es jedoch schwieriger ist, für dieses Vorgehen entsprechende Zahlenwerte abzuschätzen, sollte das oben skizzierte Vorgehen zur Ableitung eines virtuellen Szenarios verfolgt werden.

Als Bezugswert wird in Anlehnung an die Aussagen in RAC-TS eine Betriebsstunde der die Funktion ausführenden Komponente gewählt. Innerhalb dieser Stunde kann jederzeit eine Anforderung erfolgen. Es sind die Einheiten Gefährdungen je Stunde für die Gefährdungsrate,

Stunde für D und E, die einheitslose Angabe Unfälle je Gefährdung für C sowie die Angabe Opfer je Unfall für den Schaden F zu berücksichtigen.

5.8.3 Unfallszenarien

Bei quantitativen Risikoabschätzungsverfahren können unterschiedliche Unfallszenarien mit ihrer zu erwartenden Auftretenswahrscheinlichkeit berücksichtigt werden. Ein solches Vorgehen ist bei semi-qualitativen Verfahren nicht möglich. Mit dem Beispielrisikographen können Szenarien analysiert werden, die zu einer Entgleisung oder einem Zusammenstoß führen. Zur Unfallart Entgleisung werden zwei Szenarien unterschieden, zur Unfallart Zusammenstoß vier. Mit dem Beispielrisikographen kann stets nur ein Unfallszenario analysiert werden. Sind mehrere Unfallszenarien relevant oder gleichberechtigt, sind mehrere Analysen durchzuzführen. Die Ergebnisse sind entsprechend zu interpretieren oder zu verarbeiten. Dieser Arbeitsschritt ist nicht Teil der Risikographanalyse.

Eine systematische Analyse mit dem Risikographen kann durch Nutzung des Formulars in Bild 5.4 unterstützt werden. Das Formular kann zum einen für die Analyse eines einzelnen Unfallszenarios genutzt werden, zum anderen, um alle möglichen Optionen zu vergleichen. Werden z.B. die Parameterklassen für alle möglichen Szenarien ermittelt und stellt sich heraus, dass diese weitgehend übereinstimmen, so wird die Entscheidung darüber, welche Parameterklasse zur Ergebnisermittlung zu wählen ist, vereinfacht.

5.9 Parameter Schaden F

5.9.1 Grundlagen

Für den Beispielrisikographen wird in Übereinstimmung mit den Ausführungen in Abschnitt 4.9 festgelegt, dass

- eine hohe, tatsächlich im normalen Betrieb zu erwartende Schadenshöhe abzuschätzen ist,
- eine implizite Schadensschätzung vorgenommen wird,
- der Gesamtschaden basierend auf der Zahl der schwer verletzten und getöteten Personen ermittelt wird.

Im Rahmen dieser Arbeit wird ein unfallstatistikbasierter Ansatz zur Ableitung der Schadensklassen gewählt. Grundlage ist eine Betrachtung der bei einem Unfall freiwerdenden Energie. Es wird unter Ausnutzung der aus den Statistiken entnehmbaren Daten ein Zusammenhang hergestellt zwischen einer Repräsentation der von der Geschwindigkeit abhängigen (theoretisch) frei werdenden Energie, Energieäquivalent genannt, und dem zu erwartenden Schadensausmaß. Um eine möglichst intuitive Ableitung der Schadensklasse zu ermöglichen, soll dem Anwender ein Diagramm bereitgestellt werden. Ein Beispiel für ein solches Diagramm ist in Bild 5.5 dargestellt. Der Vorteil eines Diagramms ist, dass der Nutzer den Zusammenhang der in die Abschätzung des Parameters eingehenden Einflussgrößen auf die Wahl der Klasse auf den ersten Blick wahrnehmen kann. Dies ist beispielsweise bei einer tabellarischen Darstellung nicht der Fall. Die Eingangsgröße in das geplante Diagramm ist die Geschwindigkeit. Auf einer kontinuierlichen Skala, wie sie einem Anwender zur Verfügung gestellt wird, kann

Benennung der Gefährdung:						
Eingangsgrößen						
Streckengeschwindigkeit [km/h]						
Abzweiggeschwindigkeit [km/h]						
Anzahl Züge je Stunde und Abschnitt						
Blocklänge [km]						
Infrastruktur						
Wahl des Schadensparameters (lt. Diagramm)		**F_1**	**F_2**	**F_3**	**F_4**	**F_5**
ZS mit einem stehenden Zug						
ZS mit einem Zug, welcher mit der Geschwindigkeit 50 km/h fährt (Bahnhof)						
ZS mit einem Zug, welcher mit der Geschwindigkeit 80 km/h fährt (Strecke R 80)						
ZS mit einem Zug, welcher mit der Geschwindigkeit 120 km/h fährt (Strecke R 120)						
Entgleisung 75 %						
Entgleisung 25 %						
Wahl des Parameters Unfallwahrscheinlichkeit (lt. Diagramm)		**C_1**	**C_2**	**C_3**	**C_4**	
für Entgleisungen bei überhöhter Geschwindigkeit (Eingangsgröße: $v_{strecke}/v_{abzweig}$)						
für Entgleisungen, wenn Fahrweg nicht zur Verfügung steht (unstetiger Fahrweg)						
Verletzung des Folgefahrschutzes						
ZS mit einem stehenden Zug						
ZS mit einem Zug, welcher mit der Geschwindigkeit 50 km/h fährt (Bahnhof)						
ZS mit einem Zug, welcher mit der Geschwindigkeit 80 km/h fährt (Strecke R 80)						
ZS mit einem Zug, welcher mit der Geschwindigkeit 120 km/h fährt (Strecke R 120)						
Verletzung des Gegenfahrschutzes/ Flankenschutzes						
ZS mit einem stehenden Zug						
ZS mit einem Zug, welcher mit der Geschwindigkeit 50 km/h fährt (Bahnhof)						
ZS mit einem Zug, welcher mit der Geschwindigkeit 80 km/h fährt (Strecke R 80)						
ZS mit einem Zug, welcher mit der Geschwindigkeit 120 km/h fährt (Strecke R 120)						
Wahl des Parameters Gefährdungsdauer/Aussetzungszeit		**DE_1**	**DE_2**	**DE_3**		
Gefährdungsdauer (in [h], Schätzwert)						
Aussetzungszeit (in [h], aus Tabelle)						
Parameter lt. Diagramm						
Wahl des Parameters menschlicher Fehler		**MF_1**	**MF_2**	**MF_3**		
Einfache und häufig durchgeführte Aufgaben bei minimalem Stress (MF_1) Komplexere Aufgaben unter Zeitdruck, wobei eine gewisse Sorgfalt bei der Durchführung notwendig ist (MF_2) Komplexere, ungewohnte Aufgaben mit geringer Rückmeldung über den Erfolg und die Gefahr, Zerstörungen zu verursachen (MF_3)						

Bild 5.4: Formular zur Ermittlung der Parameterklassen im Rahmen der Risikographanalyse

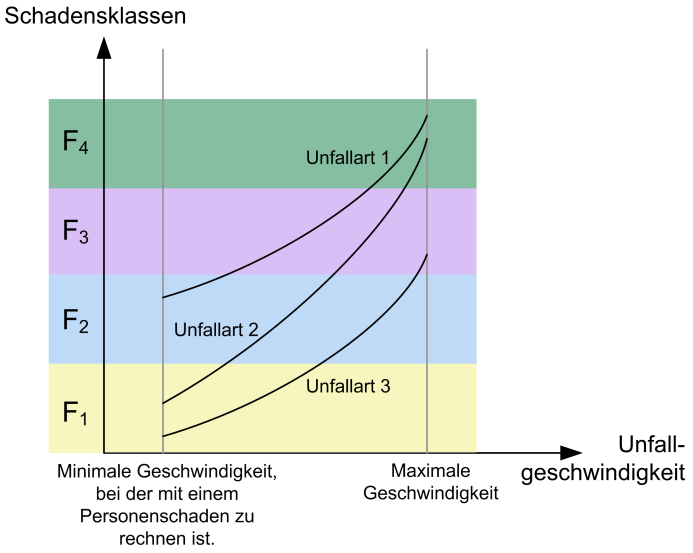

Bild 5.5: Qualitatives Beispiel für ein Diagramm zur Ableitung von Schadensklassen

er erkennen, welche Auswirkung die Festlegung der Geschwindigkeit auf die sich ergebende Klasse hat.

Es werden zunächst die drei, für eine Ableitung der Diagramme maßgeblichen, Größen Unfallart, Energieäquivalent und Unfallschaden diskutiert. Es wird ein Zusammenhang zwischen Geschwindigkeit, Unfallart und Energieäquivalent und in einem zweiten Schritt zwischen Energieäquivalent und dem aus den Statistiken entnehmbaren Schadensausmaß hergestellt. Basierend auf den Ergebnissen des zweiten Schrittes werden die Schadensklassengrenzen festgelegt.

Unfallart

Die Unfallart kann aufgrund der damit getroffenen Aussage zur Anzahl der beteiligten Fahrzeuge und deren betrieblichen Situation zur Schadensabschätzung herangezogen werden. Die maßgeblichen Statistiken erfassen nicht nur zu welchem Schaden es beim Unfall gekommen ist, sondern auch, um welche Unfallart es sich handelt. In der Verordnung EG Nr. 1192/ (2003), die bei der Erfassung von Eisenbahnunfällen zu berücksichtigen ist, werden

- Zusammenstöße (ausgenommen Unfälle an Bahnübergängen),
- Entgleisungen,
- Unfälle an Bahnübergängen,
- Unfälle mit Personenschäden, die von in Bewegung befindlichen Eisenbahnfahrzeugen verursacht wurden,
- Brände in Eisenbahnfahrzeugen und
- sonstige Unfälle

unterschieden. Für die vorliegende Betrachtung sind lediglich die beiden ersten Unfallarten relevant. Bahnübergangsunfälle werden ausgeschlossen, da sich diese hinsichtlich der Annahmen zum Schaden von den anderen Unfällen unterscheiden[2]. Die drei anderen Unfalltypen sind entweder nicht spezifisch genug oder können nicht auf Fehlfunktionen von Bahnsignalanlagen zurückgeführt werden.

Eine detaillierte Unterteilung der beiden relevanten Unfallarten wäre grundsätzlich möglich. Da jedoch für die zukünftig maßgebliche Statistik der European Railway Agency (ERA) keine anderen Unfallarten erfasst werden und es wünschenswert ist, dass die konstruktiven Annahmen des Risikographen anhand von Statistiken überprüfbar sind, wird darauf verzichtet.

Zusammenstöße sind laut UIC (2004) *Aufpralle*. In UIC (2004) werden Zusammenstöße mit einem Hindernis und Zusammenstöße mit einem anderen Zug unterschieden. In UIC (2004) werden Entgleisungen beschrieben als *Folge, wenn ein Radsatz eines fahrenden Schienenfahrzeugs unvorhergesehen aus der Spur läuft.*

5.9.2 Energieäquivalent

Die kinetische Energie eines sich bewegenden Objektes E_{kin} kann berechnet werden als

$$E_{kin} = \frac{m}{2} \cdot v^2 \tag{5.4}$$

mit m der Masse und v der Geschwindigkeit des betrachteten Objektes.

Ein fahrender Zug hat eine kinetische Energie. Im Fall eines Unfalls wird der Zug aus der aktuell gefahrenen Geschwindigkeit auf eine deutlich niedrigere Geschwindigkeit bis zum Stillstand abgebremst. Ein stehender Zug hat keine kinetische Energie. Die beim Unfall freiwerdende kinetische Energie muss laut Energieerhaltungssatz umgewandelt werden. Typisch ist, dass diese Energie zu Wärme- bzw. Reibungs- und Verformungsenergie wird. Je schneller und schwerer der Zug vor dem Unfall war, desto mehr Energie muss umgewandelt werden. Dadurch führen beispielsweise Unfälle, bei denen Züge aus hohen Geschwindigkeiten in kurzer Zeit zum Halten kommen, im Allgemeinen zu einer größeren Beschädigung des Zuges, als Unfälle, bei denen Züge aus einer niedrigeren Geschwindigkeit abgebremst werden.

Werden Unfälle betrachtet, an denen nur ein Zug (Entgleisungen) bzw. ein fahrender und ein stehender Zug (Zusammenstoß mit Hindernis) beteiligt sind, so kann die kinetische Energie entsprechend obiger Formel ermittelt werden. Wird ein Zusammenstoß zweier fahrender Züge betrachtet, so ergibt sich die gesamte kinetische Energie aus der Summe der kinetischen Energie beider Züge. Mit m_1 und m_2, der Masse der Züge, und v_1 bzw. v_2, der Geschwindigkeit der betrachteten Objekte, ergibt sich die kinetische Energie E_{kin2} zu

$$E_{kin2} = \frac{m_1}{2} \cdot v_1^2 + \frac{m_2}{2} \cdot v_2^2 \tag{5.5}$$

Ein Sonderfall sind Flankenfahrten, da die dabei freiwerdende Energie von Randbedingungen abhängig ist. Es wird der Maximalwert der kinetischen Energie angenommen, d.h. der Fall wird wie ein Zusammenstoß betrachtet.

[2]Es tritt beim Bahnübergangsunfall Personenschaden vor allem in den betroffenen Straßenfahrzeugen auf, was nicht im konstruierten Risikographen berücksichtigt wurde. Darüber hinaus spielen beim Bahnübergangsunfall u.a. die Art und Nutzung der Straße eine übergeordnete Rolle. Die Berücksichtigung dieser Einflussgrößen macht es notwendig, den Bahnübergangsunfall in einem eigenen Risikographen aufzuarbeiten und darzustellen.

Es ist zu diskutieren, ob die Betrachtung beider Parameter der Energie, Geschwindigkeit und Masse, für eine Abschätzung der Unfallfolgen notwendig ist.

In ERRI (1999) wurde ein direkter Zusammenhang zwischen Unfallgeschwindigkeit und Schadensausmaß trotz geringer Datenbasis nachgewiesen (ohne Berücksichtigung der Zugmassen). Es wird für die weitere Konstruktion davon ausgegangen, dass die Geschwindigkeit eine maßgebliche Größe zur Schadensabschätzung ist. Da die tatsächlich gefahrene Geschwindigkeit im Unfallfall im Allgemeinen nicht bekannt ist, wird als Eingangsgröße für die Schadensausmaßschätzung davon ausgegangen, dass der Zug mit der höchsten zulässigen Geschwindigkeit fährt bzw. mit einer für das betrachtete Szenario gültigen, überhöhten Geschwindigkeit. Dies ist eine Abschätzung zur sicheren Seite. Es kann davon ausgegangen werden, dass aus den betrieblichen bzw. technischen Unterlagen zu einer Strecke bzw. aus einem definierten Szenario die entsprechende Geschwindigkeit entnommen werden kann.

Die Masse der verunglückenden Fahrzeuge geht in die Berechnung der kinetischen Energie ein. Daher muss zur Berechnung der kinetischen Energie eine Aussage zur Art der beteiligten Fahrzeuge vorliegen. Der Risikograph soll so konstruiert werden, dass er möglichst für viele betriebliche Szenarien angewendet werden kann. Es gibt eine Vielzahl unterschiedlicher Eisenbahnfahrzeuge, die zu sehr unterschiedlichen Zügen zusammengesetzt werden können. Selbst bei einer Beschränkung auf typischerweise bei Nichtbundeseigenen Bahnen verkehrende Fahrzeuge ist noch eine große Zahl unterschiedlicher Fahrzeuge bzw. daraus resultierender Fahrzeugmassen zu unterscheiden. Dies kann nicht einfach und anwenderfreundlich im Risikographen abgebildet werden. Es wird deshalb der Ansatz verfolgt, dass keine Aussagen zur Masse zu machen sind, sondern die implizite Berücksichtigung der Masseverteilung der verunglückten Züge in der Statistik ausreichend ist. Bezugswert für das weitere Vorgehen ist das ohne Angaben zur Masse und unter Vernachlässigung des Faktors 0,5 zu berechnende Energieäquivalent E_{aequ} für einen bzw. zwei Züge:

$$E_{aequ} = v^2 \tag{5.6}$$

$$E_{aequ} = v_1^2 + v_2^2 \tag{5.7}$$

5.9.3 Unfallausmaß

Das Unfallausmaß wird durch die Angabe des Personenschadens beschrieben. Der Personenschaden wird berechnet zu

$$\text{Opfer} = \text{Tote} + \frac{\text{Schwerverletzte}}{10} \tag{5.8}$$

Für Fälle, in denen nur eine Gesamtzahl an verletzten Personen in der Statistik angegeben wird, muss eine Annahme bezüglich der Aufteilung in Schwer- und Leichtverletzte erfolgen. Es ist keine Literatur bekannt, der Aussagen zur zu erwartenden Aufteilung von Leicht- und Schwerverletzten im Unfallfall zu entnehmen ist. Es wird angenommen, dass ein Drittel der Personen schwer und zwei Drittel der Personen leicht verletzt wurden. Eine andere Möglichkeit der Ableitung wäre die Annahme des Faktors 10 in Übereinstimmung mit der Formel zur Berechnung eines Gesamtschadens in Abschnitt 4.9 gewesen. Das gewählte Vorgehen ist zur sicheren Seite, da es zu einem höheren Gesamtschaden führt.

Den Angaben des Personenschadens in der Literatur kann nicht notwendigerweise entnommen werden, welcher Personengruppe die Opfer angehören. Damit kann nicht sicher argumentiert werden, dass nur Reisende betrachtet werden. Eine entsprechende Einschränkung

ist daher im Rahmen der Beispielkonstruktion nicht möglich. Wenn eine aussagekräftige Statistik mit entsprechender Datenbasis zur Verfügung steht, kann eine Beschränkung des zu berücksichtigenden Schadens auf Opfer unter Reisenden erfolgen.

Eine Vielzahl von Einflüssen hat Auswirkungen auf das Schadensausmaß. Diese können z.B. unterschieden werden in Einflüsse, die auf den Grad der Zerstörung des Wagenkastens wirken, und Einflüsse, die auf die Anzahl potentieller Opfer, d.h. Anzahl der im Zug befindlichen Personen, wirken. Das vorgeschlagene Vorgehen berücksichtigt lediglich die Geschwindigkeit des Zuges bzw. der Züge und die Unfallart. Durch die vorgeschlagene Vorgehensweise, basierend auf einer Ereignisstatistik, einen Zusammenhang herzustellen zwischen den betrieblichen Bedingungen im Unfallfall und dem Schadensausmaß, erfolgt implizit eine Berücksichtigung der unterschiedlichen Einflußfaktoren auf das Schadensausmaß. Beispielsweise treten die Unfälle verteilt über alle im Netz vorhandenen Fahrzeuge auf (unterschiedliche Massen, unterschiedliche Steifigkeiten). Die betroffenen Züge haben (weitestgehend zufällig verteilt) unterschiedliche Besetzungsgrade. Diese Argumentation gilt nur, wenn die zur Verfügung stehende Statistik eine entsprechend große Datenbasis hat.

5.9.4 Geschwindigkeit, Unfalltyp und Energieäquivalent

Als Bindeglied zwischen Geschwindigkeit, Unfalltyp und Schadensausmaß wird das Energieäquivalent gewählt. Es wird davon ausgegangen, dass die Energieäquivalente von Zusammenstößen und Entgleisungen nicht vergleichbar sind, weil die Massekomponente der kinetischen Energie nicht berücksichtigt wird. Beim Zusammenstoß sind zwei Fahrzeuge beteiligt, bei einer Entgleisung im Allgemeinen nur ein Fahrzeug. Daher ist der im Energieäquivalent vernachlässigte Teil beim Zusammenstoß größer als bei einer Entgleisung. Auch ist das Verhalten der Fahrzeuge im Unfallfall nicht vergleichbar, da es sich bei einer Entgleisung eher um eine zeitlich verzögerte Energiefreigabe handelt, im Unterschied zur plötzlichen Energiefreigabe beim Zusammenstoß.

Um ein Diagramm für Zusammenstöße zu erstellen, müssen Annahmen über die Geschwindigkeiten der beteiligten Züge getroffen werden. Eine zu detaillierte Unterscheidung in den Geschwindigkeiten der beiden am Unfall beteiligten Fahrzeuge sollte nicht vorgenommen werden, da dies zum einen die Methode unübersichtlich macht und zum anderen die Aussagekraft des Ergebnisses zu sehr einschränkt. Aufgrund der Möglichkeiten des Diagramms ist die Geschwindigkeit für eines der beteiligten Fahrzeuge frei wählbar, während die Geschwindigkeit des zweiten Fahrzeugs aus vorgegebenen Szenarien zu wählen ist. Es werden vier Szenarien unterschieden.

- Zusammenstoß mit einem stehenden Zug bzw. Hindernis[3]
- Zusammenstoß mit einem Zug, welcher mit der Geschwindigkeit 50 km/h fährt (Bahnhof)
- Zusammenstoß mit einem Zug, welcher mit der Geschwindigkeit 80 km/h fährt (Strecke R 80)
- Zusammenstoß mit einem Zug, welcher mit der Geschwindigkeit 120 km/h fährt (Strecke R 120)

[3]Im Folgenden wird davon ausgegangen, dass der Fall Zusammenstoß mit stehendem Zug alle anderen Zusammenstöße mit stehenden Objekten (Hindernissen) umfasst.

		Entgleisung		Zusammenstoß			
		75%	25%	zweiter beteiligter Zug hat die Geschwindigkeit			
		Verformungsenergie		0 km/h	50 km/h	80 km/h	120 km/h
Geschwindigkeit des betrachteten Zugs [km/h]	20	300	100	400	2900	6800	14800
	40	1200	400	1600	4100	8000	16000
	60	2700	900	3600	6100	10000	18000
	80	4800	1600	6400	8900	12800	20800
	100	7500	2500	10000	12500	16400	24400
	120	10800	3600	14400	16900	20800	28800

Bild 5.6: Tabellarische Berechnung der Energieäquivalente

Flankenfahrten werden nicht gesondert betrachtet, sondern als Zusammenstöße behandelt.

Bei einer Entgleisung ist es der ungünstigste Fall, wenn der Zug durch die Entgleisung sofort zum Halten gebracht wird. In diesem Fall müsste davon ausgegangen werden, dass, unter Vernachlässigung anderer Energiebestandteile, hundert Prozent der kinetischen Energie in Verformungsenergie umgewandelt wird. In der Realität ist dieser Fall selten. Vielmehr muss angenommen werden, dass der Zug zunächst noch eine gewisse Strecke zurücklegt, dabei potentiell langsamer wird und es dann optional zu einem Personenschaden kommt. Deshalb werden für die weitere Betrachtung zwei Fälle unterschieden: Entgleisungen, bei denen 75 Prozent der kinetischen Energie in Verformungsenergie umgewandelt werden und Entgleisungen, bei denen 25 Prozent der kinetischen Energie in Verformungsenergie umgewandelt werden.

Die Berechnung der resultierenden Energieäquivalente wurde tabellarisch vorgenommen und kann Bild 5.6 entnommen werden.

5.9.5 Energieäquivalent und Schadensausmaß

Es muss ein Zusammenhang hergestellt werden zwischen der Höhe des Energieäquivalents und dem resultierenden Schadensausmaß. Dies kann anhand tatsächlicher Unfalldaten aus den relevanten Statistiken erfolgen. Das grundsätzliche Vorgehen ist

- Auswahl der für die Auswertung relevanten Unfälle,
- Berechnung des Energieäquivalents je Unfall,
- Berechnung des relevanten Gesamtpersonenschadens,
- Eintragen der Datenpunkte für jedes Datenpaar (Schadensausmaß; Energieäquivalent) in ein entsprechendes Diagramm,
- Ermittlung der Funktion (Trendlinie) der durch das Datenpaar beschriebenen Kurve.

Als Basis für die Statistikauswertung sollte eine umfangreiche, langjährige Ereignis- bzw. Unfallstatistik dienen. Parameter, die für eine Auswertung zur Verfügung stehen müssen, sind Art des Unfalls, Unfallgeschwindigkeit und Personenschaden. Eine solche Statistik stand für die Arbeit nicht zur Verfügung. Die European Railway Agency veröffentlicht auf ihrer Webseite eine *Accident Investigation notification and reports Database* (European Railway Agency (2009)), der Aussagen zu den Ereignissen in den europäischen Mitgliedsstaaten entnommen

Unfallart	Unfallort/Quelle	Unfallgeschwindigkeit	Schaden
Entgleisung	Brühl (Eisenbahnbundesamt (2000a))	ca. 122 km/h	9 T, 149 V
Entgleisung	Rheinweiler (Ritzau (1994))	140 km/h	21 T, 124 V
Entgleisung	Heilbronn 1984 (Ritzau (1994))	100 km/h	3 T, 13 SV, 44 LV
Entgleisung	Celle 1970 (Ritzau (1994))	153 km/h	5 T, 6 SV, 35 LV
Zusammenstoß	Schrozberg, (Eisenbahnbundesamt (2003))	60 km/h und 83 km/h	6T, 24 V
Zusammenstoß	Hannover (Eisenbahnbundesamt (2000b))	30 km/h und 30 km/h (geschätzt)	16 V
Zusammenstoß	Berkaer Bahnhof (Eisenbahnbundesamt (2004))	44 km/h und 39 km/h	1T, 14 SV, 13 LV
Zusammenstoß	Neufahrn (Lemke (2005))	36 km/h und 0	3 SV, 20 LV
Zusammenstoß	Aitran (Ritzau (1994))	max. 40 km/h	2 T, 6V
Zusammenstoß	Kleinfurra 1996 (Ritzau u. a. (1997))	68 km/h und 40 km/h	2 T, 12 SV
Zusammenstoß	Ansbach 1987 (Ritzau (1994))	57 km/h und 0 km/h	1 T, 52 V
Zusammenstoß	Schneverdingen 1995 (Ritzau u. a. (1997))	17 km/h und 46 km/h	102 V
Zusammenstoß	Berlin-Wannsee 1993 (Ritzau u. a. (1997))	70 km/h und 70 km/h	3T, 23 V
Zusammenstoß	Bischdorf 1994 (Ritzau u. a. (1997))	46 km/h und 0 km/h	3T, 27 V
Zusammenstoß	Bad Bramstedt 1994 (Ritzau u. a. (1997))	60 km/h und 50 km/h	7T, 80 V

Tabelle 5.2: Unfallarten-Unfallgeschwindigkeiten-Opfer

werden können. In den darin zur Verfügung stehenden Jahrgängen seit 2006 sind für das deutsche Eisenbahnwesen nur 16 Ereignisse erfasst, die im Wesentlichen im Bereich des Güterverkehrs auftraten und daher für die Arbeit nicht relevant sind. Insgesamt enthält die Datenbank weniger als 1000 Ereignisse aus allen europäischen Mitgliedsstaaten. Es ist zu diskutieren, ob als Grundlage für die Konstruktion des Risikographen alle in der Statistik erfassten Ereignisdaten berücksichtigt werden können. Da sich der Eisenbahnbetrieb in den europäischen Staaten beispielsweise im Regelwerk und Fahrzeugmaterial u.U. deutlich von den deutschen Verhältnissen unterscheidet, kann von einer Übertragbarkeit nicht ohne detaillierte Analysen ausgegangen werden. Deshalb wird ein solcher Ansatz nicht weiter verfolgt.

Die Validität des statistik-basierten Ansatzes wird an Ereignissen aus der Literatur gezeigt. Da zu diesen Ereignissen nicht nur die Unfallart und die Zahl der betroffenen Personen bekannt sein muss, sondern auch die Unfallgeschwindigkeit, ist die Zahl der verfügbaren Ereignisse gering. Eine Begrenzung auf Ereignisse aus dem Bereich Nichtbundeseigener Eisenbahnen ist nicht möglich. Eine Übersicht über die verwendeten Ereignisse findet sich in Tabelle 5.2. In der Spalte Schaden steht T für die Anzahl der Toten und SV für die Zahl der schwer verletzten Personen. Wenn nur eine Gesamtzahl an verletzten Personen angegeben ist, wurde

eine Aufteilung entsprechend dem Abschnitt 5.9.3 vorgenommen. Der Unfall in Eschede wurde bewusst von der Betrachtung ausgeschlossen, da bisherige Erfahrungen mit der statistischen Auswertung von Eisenbahnunfällen zeigen, dass der Schaden im Verhältnis zu anderen Ereignissen unverhältnismäßig hoch ist und das Diagramm statistisch verfälscht Six u. Milius (2000).

Es kann argumentiert werden, dass die in der Literatur aufgenommenen Unfälle im Allgemeinen besonders schwere Unfälle sind, da leichte Unfälle weniger öffentlichkeitswirksam sind. Implizit wird damit der Definition des zu berücksichtigenden Schadens, d.h. dass ein *ein typisches, hohes Schadensausmaß unter für das Schadensausmaß ungünstigen, jedoch betrieblich häufig und typischerweise vorkommenden Bedingungen* zu wählen ist, genüge getan.

Wenn die Unfallauswahl viele schwere Unfälle enthält, d.h. Unfälle, die bei vergleichsweise geringem Energieäquivalent zu hohem Schaden führen, so werden für die Schadensgrenzwerte niedrige zugeordnete Energieäquivalente berechnet. Bei einer Abschätzung des Schadensausmaßes anhand der betrieblichen Unfallrandbedingungen wird eine konservative Schadensklasse, d.h. eine hohe Schadensklasse gewählt. Daher ist die Auswahl von schweren Unfällen ein Vorgehen zur sicheren Seite (Bild 5.7).

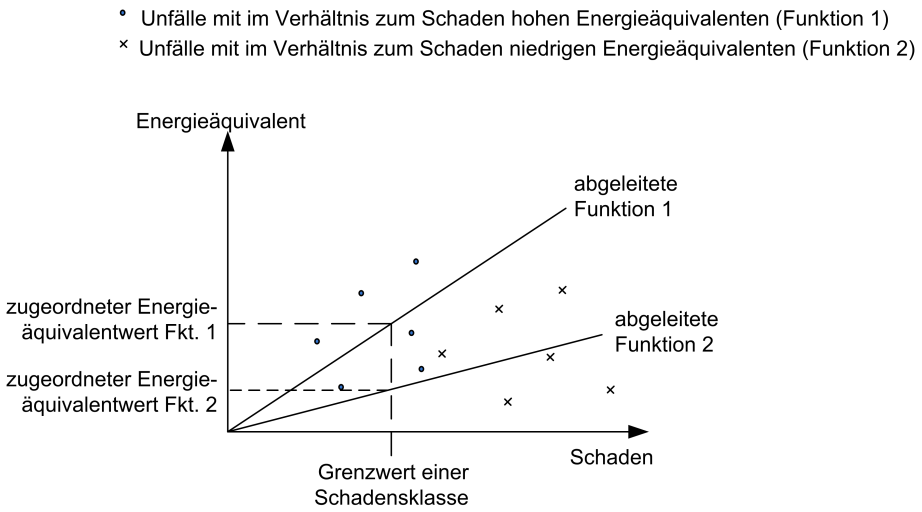

Bild 5.7: Bedeutung der Unfallauswahl auf die Schadensklassengrenzen

Erscheint es notwendig, dass Unfälle mit geringem Schadensausmaß (in Abhängigkeit des Energieäquivalents) von der Betrachtung ausgeschlossen werden, so sind zwei Vorgehen möglich: entweder ist das Datenmaterial entsprechend aufzubereiten oder bei der Ermittlung des mathematischen Zusammenhangs sind Randbedingungen zu setzen. Im ersten Fall wäre zu überlegen, dass bei mehreren zu einem Energieäquivalent gehörenden Schadensausmaßen nur diejenigen Unfälle betrachtet werden, die einen definierten, prozentualen Abstand vom Maximalwert haben. Im zweiten Fall ist die Kurve bzw. zugehörige Funktion so zu berechnen bzw. in einem zweiten Arbeitsschritt zu verschieben, dass schwere Unfälle ein höheres Gewicht bekommen. Beide Vorgehen funktionieren nur, wenn die Datenbasis ausreichend groß ist, so dass von statistisch gesicherten Ergebnissen ausgegangen werden kann.

Die mathematische Aufbereitung der Daten erfolgte vereinfacht mit dem Programm Excel. Dieses Programm erlaubt die Darstellung der Datenpunkte in einem Diagramm. Zu diesen Da-

ten kann eine sogenannte Trendlinie[4] ermittelt werden. Es stehen verschiedene Grundformen zur Verfügung. Je mehr Diagrammpunkte vorhanden sind, desto genauer bestimmbar wird die Funktion.

Die zu ermittelnde Funktion muss ausgehend von einem Punkt im Ursprung, bzw. nahe des Ursprungs langsam steigen. Der Anstieg muss mit zunehmender Schadenshöhe größer werden, da zu berücksichtigen ist, dass das Schadensausmaß nicht unbegrenzt ansteigen kann, sondern sich einem Grenzwert nähert. Es ist von einer Sättigung auszugehen, d.h. ab einer bestimmten Geschwindigkeit nimmt das Schadensausmaß nicht mehr wesentlich zu. Dies kann z.B. damit begründet werden, dass die Menge an zerstörten Fahrzeugteilen immer größer wird. Damit auch Personen in hinteren Fahrzeugen von einem Zuzsammenstoß betroffen werden, müssen die Fahrzeugteile entsprechend verschoben werden, was ab einer bestimmten Menge nur noch schwierig möglich ist. Um die Schadenssättigung statistisch nachweisen zu können, ist eine ausreichend große Datenbasis von Ereignissen notwendig.

Bei der Ableitung der Funktion im Rahmen dieser Arbeit wurde festgestellt, dass

- aufgrund der geringen Anzahl von Ereignissen eine zuverlässige Funktionsableitung nicht möglich ist,
- die von Excel zur Verfügung gestellten Trendlinien den Zusammenhang qualitativ nicht zufriedenstellend abbilden.

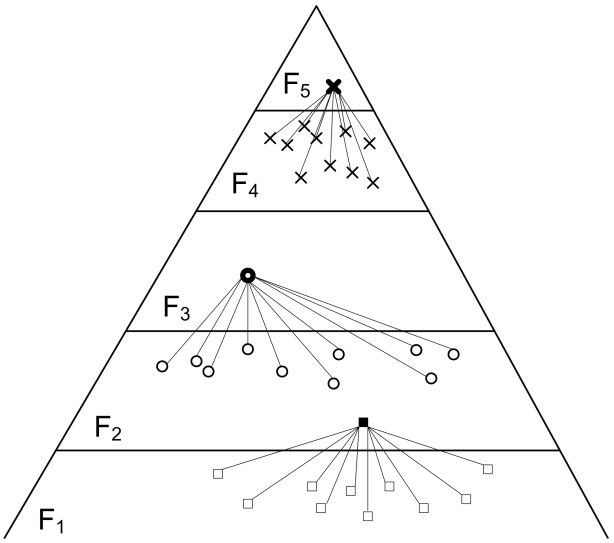

Bild 5.8: Erzeugung von Unfallereignissen

Es wurde versucht, die erste Schwierigkeit durch Anwendung von grundlegenden Überlegungen aus dem sogenannten „Eisberg“-Modell (siehe z.B. Braband (2005)) zu umgehen. Dazu wurden zunächst die Schadensklassen definiert. Es wurde angenommen, dass es zu jedem Ereignis aus der höheren Schadensklasse x mindestens 10 Ereignisse (wie in Braband (2005) beschrieben) aus der niedrigeren Schadensklasse $x-1$ gibt (siehe Beispiel in Bild 5.8).

[4]Trendlinie: Eine grafische Darstellung des Trends in Datenreihen, beispielsweise eine nach oben gerichtete Linie, die den wachsenden Umsatz über mehrere Monate hinweg darstellt. Trendlinien werden für die Erstellung von Prognosen, d.h. zur Regressionsanalyse, verwendet. (Excel (2003))

Den entsprechend zu konstruierenden Ereignissen wurde ein Schadensausmaß aus dem Schadensklassenbereich zufällig zugeteilt. Das Verfahren scheint geeignet, sich entsprechende Daten zu generieren. Trotz der Vielzahl an konstruierten Ereignissen führt die Trendlinienermittlung ebenso wie bei der Ermittlung basierend auf den wenigen Ereignissen nicht zu einem realitätsnahen Ergebnis. Die ermittelte Funktion entsprach nicht den formulierten qualitativen Anforderungen. Bei dem den Anforderungen am besten entsprechenden Ansatz verlief bis zu einer Geschwindigkeit von ca. 50 km/h die konstruierte Kurve sehr dicht an der x-Achse, deutlich unter den Datenpunkten der statistisch erfassten Ereignisse und bildete daher die Realität verzerrt ab.

Es wurde angenommen, dass eine exponentielle Funktion die Daten am besten approximieren kann. Es wurde entsprechend versucht, eine Funktion direkt aus den Datenpunkten abzuleiten. Dies war nicht zielführend, da sich die Parameter der Formel nicht entsprechend der qualitativen Vorgaben anpassen ließen. Eine rein exponentielle Funktion scheint nicht geeignet für die Approximation zu sein.

Es wird im Rahmen der Arbeit daher näherungsweise angenommen, dass der erste Teil der Kurve durch eine lineare Funktion abgebildet werden kann und der zweite Teil der Kurve durch eine exponentielle Funktion. Die entsprechenden Wertebereiche ergeben sich aus dem Schnittpunkt beider Kurven.

Die Diagramme sind so zu erstellen, dass der gesamte für einen Analyse potentiell relevante Bereich der Energieäquivalente abgedeckt wird. Für Zusammenstöße ist der Zusammenstoß von zwei Fahrzeugen mit Maximalgeschwindigkeit 120 km/h maßgeblich. Es ergibt sich ein Energieäquivalentwert von 28800. Für Entgleisungen wird angenommen, dass ein Zug mit überhöhter Geschwindigkeit fährt. Es wird von einer Geschwindigkeit von 140 km/h ausgegangen. Es ergibt sich ein Energieäquivalentwert von 19600.

In den Bildern 5.9 und 5.10 sind die Diagramme mit den Datenpunkten sowie den linearen und exponetiellen Trendlinien angegeben.

Mit sich verändernder Datenbasis wird sich auch die Funktion des Schadens verändern. Es ist anzustreben, der Auswertung eine möglichst breite Datenbasis zu Grunde zu legen. Aufgrund der geringen Anzahl von Fällen werden die Unfalldaten nicht statistisch analysiert. Wenn eine größere Datenbasis zur Verfügung steht, können die Daten hinsichtlich z.B. des Konfidenzintervalls ausgewertet werden.

5.9.6 Ableitung von Schadensklassengrenzen

Um eine Schadensklasse als Ergebnis der Beurteilung zu erhalten, wählt der Anwender die Unfallgeschwindigkeit und den zu erwartenden Unfalltyp. In einem Diagramm kann der Anwender die Schadensklasse ablesen. Eine detaillierte textuelle Beschreibung der Schadensklasse ist nicht notwendig. Dies hat den Vorteil, dass Missverständnisse und unnötige Diskussionen vermieden werden.

Gefahrenstufe	Konsequenzen für Personen
katastrophal	Unfalltote und/oder zahlreiche Schwerverletzte
kritisch	einzelner Unfalltoter und/oder Schwerverletzter
marginal	kleinere Verletzung
unbedeutend	mögliche geringfügige Verletzung

Tabelle 5.3: Gefahrenstufen nach DIN EN 50126 (2000)

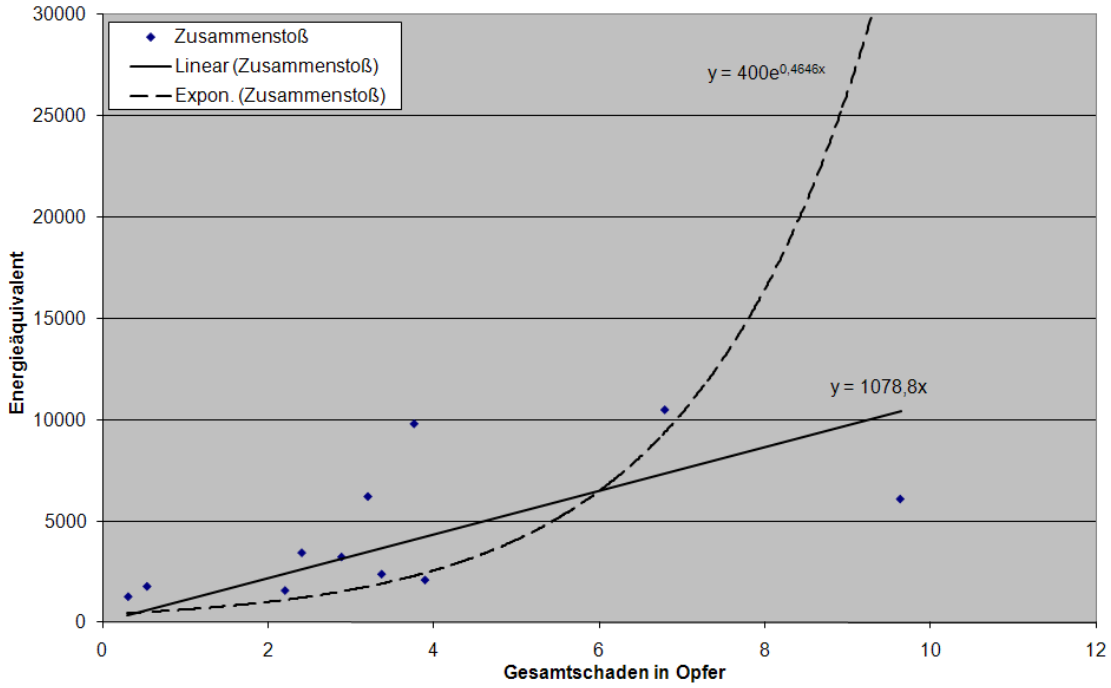

Bild 5.9: Darstellung des Zusammenhangs von Energieäquivalent und Schadensausmaß für Zusammenstöße

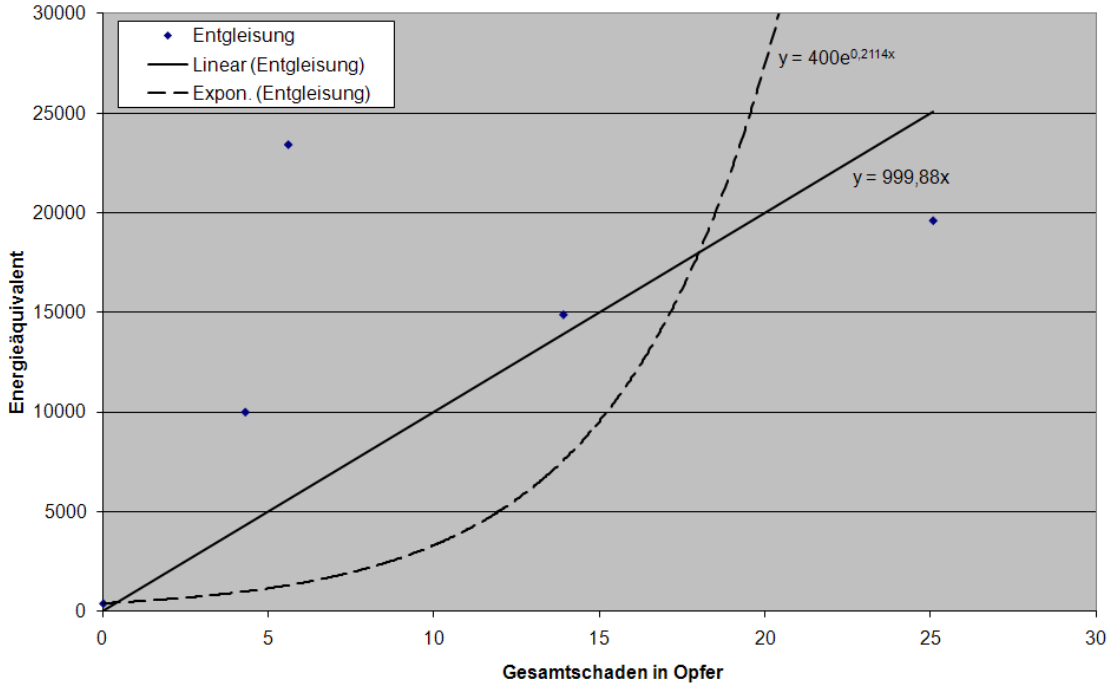

Bild 5.10: Darstellung des Zusammenhangs von Energieäquivalent und Schadensausmaß für Entgleisungen

In DIN EN 50126 (2000) werden beispielhafte Schadensklassenbeschreibungen gegeben (siehe Tabelle 5.3 in dieser Arbeit). Da für den zu konstruierenden Risikographen ausschließlich Personenschaden betrachtet wird, kann der in der Norm angegebene Umweltschaden nicht berücksichtigt werden. Die Erfahrung zeigt, dass im Eisenbahnwesen häufig Situationen konstruiert werden können, bei denen es zu Unfalltoten kommt. Dies würde bedeuten, dass in sehr vielen Fällen eine Schadensklassifikation als katastrophal erfolgt. Die Bandbreite der Klassen ist, wird die Formel zur Berechnung eines Gesamtschadens zu Grunde gelegt, groß und für die einzelnen Klassen unterschiedlich. Aus diesen Gründen wird die in DIN EN 50126 (2000) gegebene Schadensklassenfestlegung nicht übernommen. Für den zu erstellenden Risikographen werden die Schadensklassengrenzen durch den Konstrukteur festgelegt.

Ein Kriterum bei der Schadensklassendefinition ist, dass aufgrund der Abhängigkeiten des Risikomodells der Abstand der Klassengrenzen untereinander gleichbleibend sein sollte. Der Faktor 10, welcher zwischen den Ergebnisklassengrenzen liegt, führt bei der Beschreibung des Gesamtschadens zu einer zu undetaillierten Einteilung. Es wird als Faktor zwischen den einzelnen Klassengrenzen der Faktor $\sqrt{10}$ gewählt. $\sqrt{10}$ ist geeignet für die Ermittlung der Schadensklassengrenzen, da 10 eine Potenz von $\sqrt{10}$ ist und somit eine systematische Ergebnisableitung möglich ist. Es ist zu beachten, dass der gleichbleibende Faktor zwischen den tatsächlich in die Risikoformel eingehenden Parameterklassengrenzen, d.h. den Schadensgrenzen, gelten muss, nicht zwischen den Energieäquivalentklassengrenzen.

Die ermittelten Unfalldaten zeigen, dass es eine Häufung von Gesamtschaden im Bereich zwischen drei und fünf Opfern gibt. Es erscheint sinnvoll, eine Schadensklasse durch den Maximalwert dieser Häufung, den Gesamtschaden von fünf Opfern, zu begrenzen. Einige Ereignisse, die laut DIN EN 50126 (2000) als katastrophal eingruppiert werden müssten, da sie zu mehr als einem Opfer führen, fallen bei dem hier verfolgten Ansatz nicht in die höchste Schadensklasse. Wie bereits argumentiert wurde, geben die Daten aus der Literatur einen hohen, unter ungünstigen Bedingungen möglichen Schaden wieder. Laut Eisberg-Modell (Braband (2005)) gäbe es zu jedem Ereignis mit einem Schaden zwischen einem und fünf Opfern eine Vielzahl von Ereignissen gleicher Ursache, die mit deutlich geringerem Schadensausmaß aufgetreten sind. Die Norm DIN EN 50126 (2000) gibt nicht an, für welches Szenario die angegebenen Werte gelten. Nur mit einer solchen Angabe ist die Anwendung der gegebenen Schadensklassen möglich. Soll beispielsweise laut Norm die Beurteilung des Schadens für den worst-case erfolgen, so kann vermutet werden, dass jede Gefährdung das Potential für einen nach DIN EN 50126 (2000) katastrophalen Unfall hat. Ein solches Vorgehen ist nicht zielführend. Wird interpretiert, dass die Norm einen mittleren Schaden betrachtet, so kann vermutet werden, dass ein solches Vorgehen näherungsweise mit dem in dieser Arbeit verfolgten Ansatz übereinstimmt.

Eine qualitative Begründung für den in dieser Arbeit gewählten Grenzwert ist, dass damit zwischen Ereignissen, mit einer geringen Opferzahl und einer größeren Häufigkeit, die nur lokale Aufmerksamkeit erfahren[5] und Ereignissen, die aufgrund einer höheren Opferzahl überregionale Aufmerksamkeit erfahren, unterschieden werden. Dieses Argument berücksichtigt den Imageschaden des Unternehmens Bahn durch einen Unfall.

Die weiteren Schadensklassengrenzen ergeben sich durch Anwendung des Faktors $\sqrt{10}$. Es ist im Rahmen der Schadensklassenfestlegung notwendig zu entscheiden, welche minimalen und maximalen Werte abgedeckt werden sollen. Bei der Festlegung der minimalen Schadensklassen-

[5]Dies kann unter Umständen damit begründet werden, dass ein entsprechendes niedriges Schadensausmaß häufig bei Bahnübergangsunfällen auftritt. Da Bahnübergangsunfälle relativ häufig sind, ist eine gewisse Gewöhnung in der Gesellschaft zu vermuten.

Grenzwert	$\frac{5}{\sqrt{10}^3}$	$\frac{5}{\sqrt{10}^2}$	$\frac{5}{\sqrt{10}}$	5	über 5
	f	$\sqrt{10}f$	$10f$	$10\sqrt{10}f$	
equ. Opfer bis	0,158	0,5	1,58	5	
Schadensklassen	F_1	F_2	F_3	F_4	F_5

Tabelle 5.4: Schadensklassengrenzen

grenze ist auf einen sinnvollen Detaillierungsgrad und die Relevanz der entsprechenden Klasse für die Bewertung zu achten. Es wird in der Beispielkonstruktion der Wert von 0,158 Opfern als Grenze der niedrigsten Schadensklasse gewählt. Eine Klasse mit noch geringerem Grenzwert wäre möglich gewesen. Der von der so begrenzten Klasse abgedeckte Schadensbereich liegt jedoch in einem so niedrigen Bereich, dass eine Differenzierung im zugrunde liegenden Diagramm nicht möglich ist. Der Grenzwert der obersten Schadensklasse ergibt sich aus der Anwendung von RAC-TS. Die Berechnung der Klassengrenzen erfolgt in Tabelle 5.4.

Eine wesentliche Eingangsgröße in die Konstruktion des Schadensparameters für den Risikographen sind reale Unfalldaten. Da diese im Rahmen der Arbeit nicht zur Verfügung gestellt wurden, mussten veröffentlichte Unfalldaten herangezogen werden. Dadurch steht nur wenig Datenmaterial zur Verfügung. Es wird empfohlen, den Zusammenhang zwischen den Unfallarten, den Energieäquivalenten und dem Schadensausmaß regelmäßig zu prüfen und, wenn möglich, die Datenbasis deutlich zu vergrößern. Dies wird zur Folge haben, dass sich die Berechnung der Trendlinie verändert und sich damit die den Schadensgrenzwerten zugeordneten Energieäquivalente ändern. Inwieweit eine Veränderung der Grenzwerte notwendig wird, muss geprüft werden.

Klasse	Gesamtschaden bis	Energieäquivalentgrenzwert	
		Zusammenstoß	Entgleisung
F_1	0,158	171	158
F_2	0,500	539	500
F_3	1,581	1706	1581
F_4	5,000	5394	4999
F_5	mehr als 5		

Bild 5.11: Zuordnung der Schadensklassen zu den Energieäquivalent-Grenzwerten

Mit Hilfe der im vorherigen Abschnitt ermittelten Gleichungen für die Trendlinien können Energieäquivalenzwerte zu den Schadensklassengrenzwerten berechnet werden (siehe Abbildung 5.11). Zur Berechnung der Grenzwerte ist nur der lineare Teil der Funktion zu berücksichtigen, da der Schnittpunkt der beiden Trendlinientypen bei ca. 6 bzw. 18 Opfern und damit deutlich über dem höchsten Schadensklassengrenzwert liegt.

Die Diagramme zur Ermittlung der Parameterklasse für den Schaden werden wie folgt erstellt:

- Es wird ein Diagramm erzeugt. Auf der x-Achse ist die Geschwindigkeit des betrachteten Fahrzeugs abzutragen, auf der y-Achse das Energieäquivalent.

- Für die gewählten Szenarien (d.h. die Entgleisungen mit unterschiedlicher Energiefreisetzung, bzw. die Zusammenstöße mit unterschiedlichen Geschwindigkeitsscheren) werden

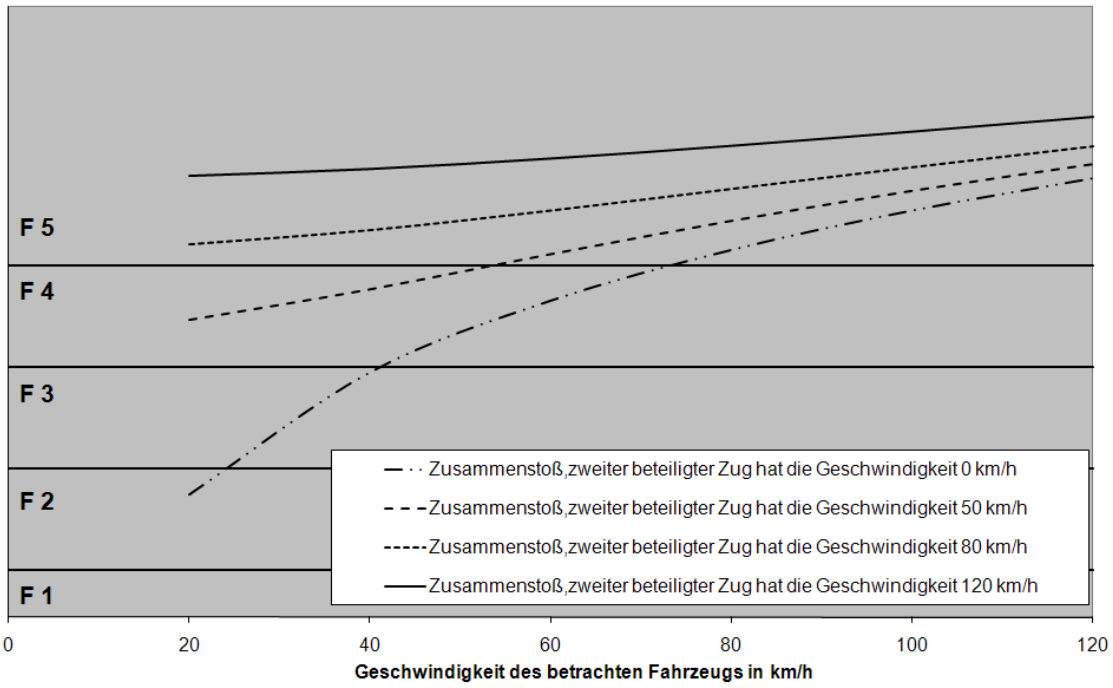

Bild 5.12: Diagramm zur Ermittlung der Schadensklassengrenzen bei Zusammenstößen

die Energieäquivalente basierend auf der Geschwindigkeit des betrachteten Fahrzeugs ermittelt.

- Mit Hilfe der Daten können die Kurven für die einzelnen Szenarien in dem Diagramm erzeugt werden
- Entsprechend der ermittelten Energieäquivalentwerte werden horizontale Linien in das Diagramm eingefügt, die die einzelnen Schadensklassen voneinander trennen.
- Dem Anwender wird das Diagramm ohne eine Beschriftung der y-Achse zur Verfügung gestellt, da diese Information für die Anwendung des Diagramms nicht notwendig ist. Die Beschriftung der Schadensklassen erfolgt auf der Diagrammfläche.

Die sich ergebenden Diagramme sind in Abbildung 5.12 bzw. 5.13 dargestellt.

5.10 Parameter Unfallwahrscheinlichkeit C

5.10.1 Einleitung

Im Abschnitt 4.10 wurde diskutiert, dass für den Risikographen mittlere, typische Reduktionsmöglichkeiten abzuschätzen sind. Die Wirkung der Reduktionsfaktoren wird in einer Unfallwahrscheinlichkeit angegeben.

Reduktionsfaktoren können nicht anhand von betrieblichen Daten berechnet und aufgrund der Vielzahl unterschiedlicher Einflüsse nicht anhand realer Daten verifiziert werden. Deshalb kann das Erstellen eines Diagramms zur Ableitung von Unfallwahrscheinlichkeitsklassen nur

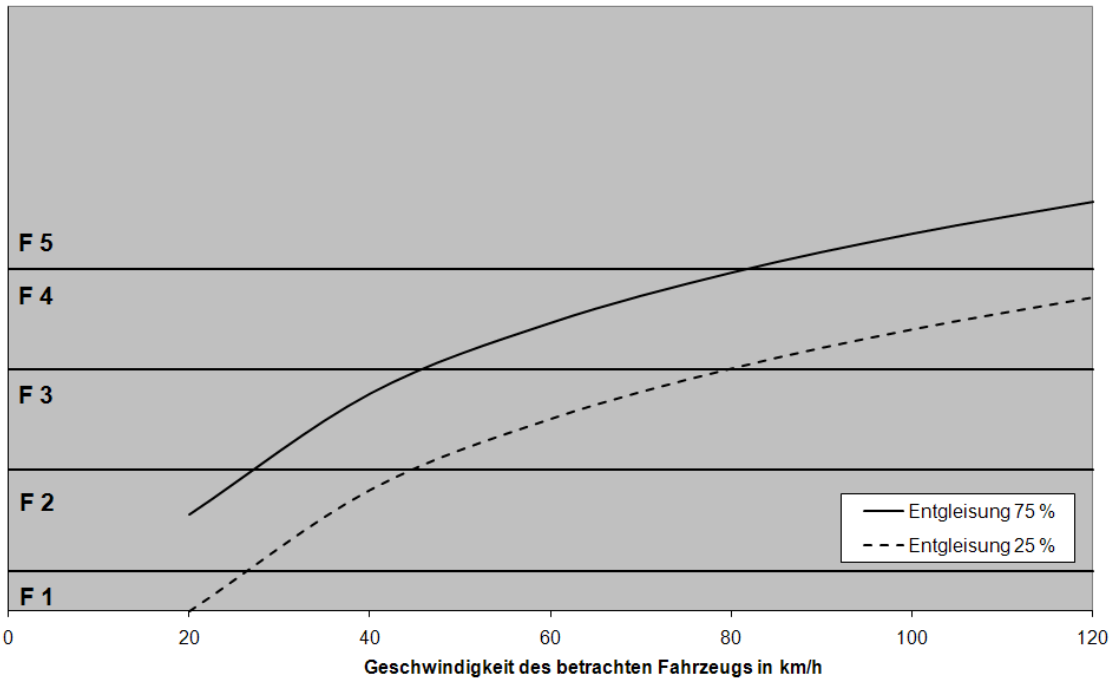

Bild 5.13: Diagramm zur Ermittlung der Schadensklassengrenzen bei Entgleisungen

durch theoretische Überlegungen zum Bahnbetrieb, ggf. unterstützt von Expertenwissen, erfolgen. Dabei ist zwischen den unterschiedlichen Arten von Reduktionsfaktoren (siehe Abschnitt 4.10) zu unterscheiden:

- physikalische Schutzmaßnahmen, wie technische Diagnose-, Warn-, Kontroll- und Schutzsysteme,
- verfahrenstechnische Schutzmaßnahmen, wie Regeln, Verfahren und Prozesswissen der Bediener,
- sich aus bestimmten Umständen (insbesondere hemmenden betrieblichen Randbedingungen) ergebende Schutzmaßnahmen, wie ungeplante, aber dennoch vorteilhafte Umstände, die einen Unfall verhindern oder abwehren können.

Physikalische Schutzmaßnahmen, vorteilhafte Umstände

Für diese Arbeit wird davon ausgegangen, dass physikalische Maßnahmen nicht im Rahmen der Reduktionsfaktoren zum Ansatz gebracht werden. Die Wahrscheinlichkeit, dass zwei technische Komponenten versagen, wird als so niedrig angesehen, dass die Genauigkeit der Risikoabschätzung mit dem Risikographen nicht ausreichend ist.

Es werden keine zufälligen, ggf. vorteilhaften Einflüsse aus z.B. der Umgebung berücksichtigt. Es wird davon ausgegangen, dass die Bahnanlagen sowie die Umgebung der Bahnanlagen richtlinienkonform sind.

Verfahrenstechnische Maßnahmen

Im Rahmen der verfahrenstechnischen Maßnahmen ist das Handeln der beteiligten Personen zu berücksichtigen. Für das Eisenbahnwesen kann unterschieden werden in Betriebspersonal im Zug und außerhalb des Zuges, anderen Personen im Zug sowie Dritten ausserhalb des Zuges.

Da in einem modernen Eisenbahnsystem aufgrund dessen Komplexität und der zunehmenden Zentralisierung der Betriebsführung nur noch wenig Personal von außerhalb des Zuges direkt auf den Zug einwirken kann, wird nur der Fahrdienstleiter betrachtet. Aufgrund der hohen psychischen Belastung des Fahrdienstleiters aufgrund seiner Aufgaben in einem modernen Stellwerk bzw. einer Betriebszentrale, des auf den Displays vermittelten, verdichteten Informationsgehalts und der großen Entfernung von den zu steuernden Eisenbahnanlagen kann nicht davon ausgegangen werden, dass der Fahrdienstleiter eine Gefährdung rechtzeitig erkennt. Der Fahrdienstleiter wird deshalb als Reduktionsfaktor nicht berücksichtigt.

Es wird davon ausgegangen, dass der Zugführer oder weitere, sich in den Wagen aufhaltende, Personen bei einer Fehlfunktion der Bahnsignalanlagen keinen Einfluss auf den Betrieb nehmen können.

Das maßgebliche Personal im Zug ist der Triebfahrzeugführer. Die Wahrscheinlichkeit, dass der Triebfahrzeugführer eine Gefährdung erkennen und aufgrund seiner Maßnahmen ein Ereignis verhindern kann, ist abhängig von verschiedenen Einflüssen, aber im Besonderen von der Art der Gefährdung und dem Zeitfenster, welches zwischen Auftreten bzw. Erkennen der Gefährdung und einem potentiellen Unfall für eine Handlung zur Verfügung steht. Zur Ermittlung des Zeitfensters für den Triebfahrzeugführer sind betriebliche Einflüsse zu berücksichtigen.

5.10.2 Ableitung von Grenzwerten

Für den Risikographen werden nur wenige unfallverhindernde Einflüsse berücksichtigt. Es kann davon ausgegangen werden, dass in der Praxis weitere Faktoren zur Unfallvermeidung beitragen, so dass die tatsächliche Unfallwahrscheinlichkeit geringer ist als die abgeschätzte Unfallwahrscheinlichkeit. Daher ist davon auszugehen, dass durch das genannte Vorgehen eine zu hohe Unfallwahrscheinlichkeit in den Risikographen eingeht. Dies führt zu Ergebnissen auf der sicheren Seite. Der Effekt tritt gleichmäßig bei allen Risikoabschätzungen auf. Die getroffenen Annahmen führen dazu, dass der Reduktionsfaktor (mindestens) wie gefordert *mittlere, durchschnittliche (typische) Reduktionsmöglichkeiten* beschreibt.

Für den Zusammenhang von z.B. betrieblichen Größen und Unfallwahrscheinlichkeit gibt es keine ausagekräftigen Statistiken. Alle Grundlagen für die Konstruktion der Diagramme zur Ermittlung der Unfallwahrscheinlichkeit beruhen auf Abschätzungen. Daher sollte der Detaillierungsgrad der Klassengrenzwerte nicht zu hoch sein, um nicht eine Genauigkeit vorzutäuschen, die nicht gegeben ist.

Berechnung	bis $\frac{100}{\sqrt{10}^3}$	$\frac{100}{\sqrt{10}^2}$	$\frac{100}{\sqrt{10}}$	100
oberer Grenzwert (gerundet)	3	10	30	100
Klasse	C_1	C_2	C_3	C_4

Tabelle 5.5: Unfallwahrscheinlichkeitsgrenzwerte für Reduktionsfaktorklassen (gerundet)

Die Berechnung der Unfallwahrscheinlichkeitsklassengrenzwerte wird mit 100 Prozent Unfallwahrscheinlichkeit begonnen. Der Abstand der Grenzwerte wird in Anlehnung an das Vor-

gehen bei der Ermittlung der Schadensklassengrenzwerte mit dem Faktor $\sqrt{10}$ ermittelt (Tabelle 5.5). Der Abstand der einzelnen Klassengrenzen ist relativ groß. Alle Ereignisse, deren Unfallwahrscheinlichkeit größer als 30 Prozent ist, werden in einer Klasse zusammengefasst. Es wird darauf verzichtet, eine noch detailliertere Aufteilung vorzunehmen, da sich diese nicht im Ergebnis niederschlagen würde.

Die Ermittlung der Unfallwahrscheinlichkeit erfolgt getrennt für die Unfallarten Entgleisung und Zusammenstoß. Als Basis der Ableitung wird der Betrieb auf der freien Strecke angenommen. Für Szenarien im Bahnhof gelten grundsätzlich die gleichen Überlegungen.

5.10.3 Unfallwahrscheinlichkeit einer Entgleisung

Laut Maschek (2009) liegen Ursachen für eine Entgleisung in Fehlern bei der Sicherung beweglicher Fahrwegelemente, was zu unstetigen Stellen im Fahrweg führt, d.h. dass der Fahrweg nicht zur Verfügung steht. Darüber hinaus können in einem stetigen Fahrweg auch zu hohe Geschwindigkeitsvorgaben oder Fehler bei der Regelung und Überwachung der Geschwindigkeit zu Entgleisungen führen.

Die Möglichkeit, eine Entgleisung nach Auftreten einer Fehlfunktion zu verhindern, ist von einer Vielzahl von Randbedingungen abhängig. Es wird abgeschätzt, dass aufgrund der Schwierigkeit für den Triebfahrzeugführer, unstetige Stellen im Fahrweg und falsche betriebliche Angaben zu erkennen, dieser kaum Einfluss auf die Unfallwahrscheinlichkeit hat. Es ist eine Abschätzung zur sicheren Seite, die Möglichkeiten zur Unfallvermeidung durch den Triebfahrzeugführer nicht zu berücksichtigen.

Für Entgleisungen aufgrund zu hoher Geschwindigkeit kann davon ausgegangen werden, dass die Geschwindigkeitsdifferenz zwischen gefahrener und zulässiger Geschwindigkeit maßgeblich für die Unfallwahrscheinlichkeit ist. Der Infrastruktur sind Sicherheitspuffer inhärent, d.h. es kommt nicht bereits bei minimalen Geschwindigkeitsüberschreitungen zu einem Unfall. In Schramm (1962) wird abgeschätzt, dass eine Entgleisung begünstigt wird, wenn ein Fahrzeug mit zu hoher Geschwindigkeit in einen Kreisbogen mit kleinem Halbmesser ohne Übergangsbogen einfährt. Eine exakte Berechnung der Entgleisungsgeschwindigkeit ist von verschiedenen fahrzeug- und infrastrukturabhängigen Faktoren abhängig. Überschlägig kann nach Schramm (1962) die Entgleisungsgeschwindigkeit V_{entgl} berechnet werden zu

$$V_{entgl} \geq 5 \cdot \sqrt{R} \tag{5.9}$$

mit V_{entgl} in km/h und Radius R in m. In Bild 5.14 sind die in Schramm (1962) berechneten Entgleisungsgeschwindigkeiten den nach Richtlinie 800 (1997) zulässigen Abzweiggeschwindigkeiten für Weichen gegenübergestellt. Es wird im Weiteren davon ausgegangen, dass ein Zug entgleist, wenn er mit dem 1,7fachen der zulässigen Geschwindigkeit einen Bogen durchfährt.

Die folgenden Arbeitsschritte beschreiben die Konstruktion des Diagramms:

- In dem zu erstellenden Diagramm wird auf der x- und auf der y-Achse die Geschwindigkeit abgetragen. Auf der x-Achse wird die zulässige Geschwindigkeit des Fahrzeugs, auf der y-Achse die gefahrene Geschwindigkeit des Fahrzeugs abgetragen.

- Es wird angenommen, dass die Unfallwahrscheinlichkeit beim Einhalten der zulässigen Geschwindigkeit null ist, beim 1,7fachen der zulässigen Geschwindigkeit 100 Prozent beträgt.

Halbmesser der Weiche	Entgleisungs-Geschwindigkeit	zul. Geschwindigkeit lt. DB-Konzernrichtlinie 800.0120 für einfache Weichen mit geradem Herzstück/ Bogenherzstück	Faktor
190	69	40	1,725
300	86	50	1,72
500	111	60	1,85
760	138	80	1,725
1200	173	100	1,73

Bild 5.14: Gegenüberstellung der in Schramm (1962) berechneten Entgleisungesgeschwindigkeiten mit den zulässigen Geschwindigkeiten nach Richtlinie 800 (1997)

- Die Festlegung der Parameterklassengrenzen erfolgt anhand der in Tabelle 5.5 gegebenen Zahlenwerte. Dazu wird der Abstand zwischen der einfachen und der 1,7fachen zulässigen Geschwindigkeit proportional zu den Grenzwerten aufgeteilt.

Für Fehlfunktionen, die zu unstetigen Stellen im Fahrweg führen, muss davon ausgegangen werden, dass es sicher zu einer Entgleisung kommt. Es muss die höchste Klasse gewählt werden. Ein entsprechender Verweis befindet sich im Diagramm (Bild 5.15).

5.10.4 Unfallwahrscheinlichkeit eines Zusammenstoßes

Ein Zusammenstoß kann auftreten, wenn die betrieblichen Maßnahmen, mit denen Eisenbahnfahrzeuge auf Abstand gehalten werden (Folge- und Gegenfahrschutz, Flankenschutz) versagen (siehe Maschek (2009)). Auch die in Maschek (2009) genannten Aufpralle, deren Ursache in einem nicht vorhandenen Schutz vor externen Objekten liegt, werden im Rahmen der Arbeit unter den Zusammenstößen erfasst. Die Ursachen für die genannten Unfälle können sehr unterschiedlich sein.

Es wird bei der Entwicklung von der Gefährdung zum Zusammenstoß davon ausgegangen, dass nur der Triebfahrzeugführer nach Auftreten der Gefährdung einen Unfall verhindern kann. Maßgeblich ist die gefahrene Geschwindigkeit des Zuges. Je höher die Geschwindigkeit, desto geringer ist bei gleichbleibender Sichtweite das Zeitfenster, welches für Maßnahmen des Triebfahrzeugführers zur Verfügung steht, da der Abstand zu einem anderen Zug bzw. auf ein Hindernis sich entsprechend schneller verringert. Die Wahrscheinlichkeit, dass es zu einem Zusammenstoß kommt, wird als Zusammenstoßwahrscheinlichkeit bezeichnet.

Wenn sich zwei Züge im gleichen Abschnitt bzw. benachbarten Abschnitten befinden, so ist die Unfallwahrscheinlichkeit bei Verletzungen des Folgefahrschutzes maßgeblich davon abhängig, wie sich die Geschwindigkeiten der Züge zueinander verhalten. Dieser Sachverhalt wird in der Konfliktwahrscheinlichkeit abgebildet. Die Unfallwahrscheinlichkeit ergibt sich aus dem Produkt von Konfliktwahrscheinlichkeit und Zusammenstoßwahrscheinlichkeit.

Im Folgenden wird zunächst betrachtet, wie wahrscheinlich ein Unfall nach Auftreten der Gefährdung ist (Zusammenstoßwahrscheinlichkeit). In einem zweiten Schritt wird analysiert,

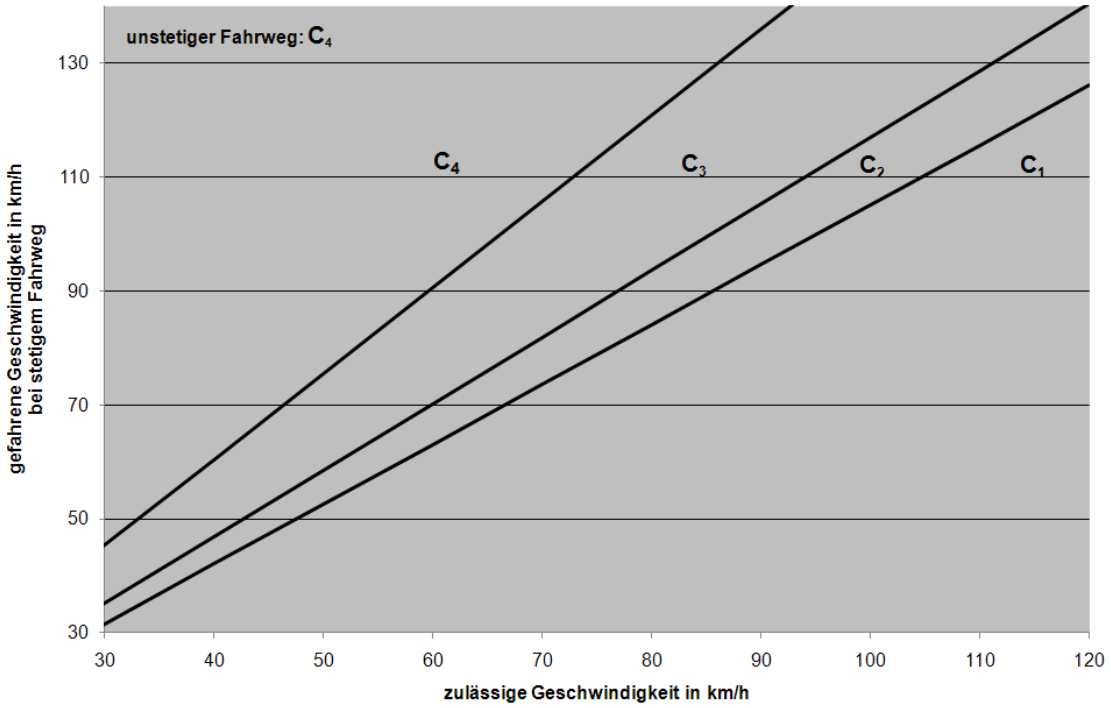

Bild 5.15: Diagramm zur Ermittlung der Unfallwahrscheinlichkeit für Entgleisungen

welche Auswirkung das Verhältnis der Geschwindigkeiten der beiden relevanten Züge hat (Konfliktwahrscheinlichkeit).

Wenn eine Fehlfunktion zu einem Versagen von Folge- oder Gegenfahrschutz, Flankenschutz oder dem Schutz vor externen Hindernissen führt, liegen unterschiedliche betriebliche Situationen vor, die maßgebliche Rückwirkung auf die Reduktionsfaktoren haben.

- Folgefahrschutz: Wenn eine Fehlfunktion zu einem Versagen des Folgefahrschutzes führt, so können sich zwei Züge in einem Block bzw. auf einer Fahrstraße befinden. Im Unterschied zu Verletzungen des Gegenfahrschutzes bewegen sich die Züge in eine Richtung. Es kann nur zu einem Unfall kommen, wenn der zweite, d.h. der von der Fehlfunktion betroffene Zug schneller fährt als der erste Zug. Nur der Triebfahrzeugführer des zweiten Zuges kann durch angemessenes Verhalten (Reduzierung der Geschwindigkeit bzw. sofortiger Halt) einen Unfall verhindern.

- Gegenfahrschutz: Wenn eine Fehlfunktion zu einem Versagen des Gegenfahrschutzes führt, so fahren zwei Züge aufeinander zu. Die Triebfahrzeugführer beider Züge müssen versuchen, durch ihr Verhalten (d.h. bremsen, wenn gefährliche Situation erkannt wird) in Abhängigkeit der betrieblichen Randbedingungen einen Unfall zu verhindern. Die Unfallwahrscheinlichkeit kann berechnet werden unter der Annahme, dass die Triebfahrzeugführer beider Züge versuchen, innerhalb der Sichtentfernung voreinander zum Halten zu kommen.

- Flankenschutz: Wenn eine Fehlfunktion zu einem Versagen des Flankenschutzes führt, so besteht die Möglichkeit, dass der von der Fehlfunktion betroffene Zug einem anderen

Zug in die Flanke fährt. Es ist davon auszugehen, dass nur der Triebfahrzeugführer des in die Flanke fahrenden Zuges die Möglichkeit hat, zur Unfallvermeidung beizutragen. Die Unfallwahrscheinlichkeit wird ermittelt, indem geprüft wird, ob der in die Flanke fahrende Zug innerhalb der angenommenen Sichtentfernung zum Halten kommt.

- Schutz vor externen Objekten: Wenn eine Fehlfunktion zu einem Versagen des Schutzes vor externen Objekten führt, so kann nur der Triebfahrzeugführer des betroffenen Zuges durch angemessene Reaktion einen Unfall verhindern. Die Unfallwahrscheinlichkeit ist im Wesentlichen abhängig von der gefahrenen Geschwindigkeit und der Sichtentfernung zum externen Objekt.

Es wird zunächst die Zusammenstoßwahrscheinlichkeit bei Verletzung des Folgefahrschutzes untersucht. Es wird für die Betrachtung davon ausgegangen, dass der von der Fehlfunktion betroffene Zug mit Streckengeschwindigkeit fährt (Annahme: 120 km/h). Der Zug wird als Zug 2 bezeichnet (Bild 5.16).

Bild 5.16: Begriffsvereinbarung für Verletzungen des Folgefahrschutzes

Die Wahrscheinlichkeit, dass es zu einem Unfall kommt, wenn sich ein Fahrzeug auf ein anderes zu bewegt, ist maßgeblich abhängig von der Sichtentfernung, der Reaktionszeit t_R und der Geschwindigkeit des Fahrzeugs v_0. Es sind die während Reaktions- und Bremszeit zurückgelegten Wege dem Abstand zum anderen Fahrzeug gegenüberzustellen. Es wird von einer Sichtentfernung von 300 Metern ausgegangen und es werden durchschnittliche (typische) Sichtbedingungen angenommen. Es wird von einer maximalen Bremsverzögerung a_{beschl} von 2 $\frac{m}{s^2}$ sowie einer Reaktionszeit von 2 Sekunden ausgegangen. Die während der Reaktionszeit zurückgelegte Strecke s_R berechnet sich zu $s_R = v_0 * t_R$. Die während des Bremsens zurückgelegte Strecke s_B berechnet sich zu $s_B = 0,5 * v_0^2 * a_{beschl}^{-1}$. Es kommt zu einem Zusammenstoß, wenn die Summe aus Brems- und Reaktionsstrecke des Fahrzeugs größer als die zur Verfügung stehende Sichtstrecke von 300 Metern ist. Zur Berechnung der Wahrscheinlichkeit wird angesetzt, dass bei einem negativen ermittelten Abstand es sicher zu einem Unfall kommt (Wahrscheinlichkeit eins) und bei einem Abstand von 300 Metern (Fahrzeug 2 steht) es sicher nicht zu einem Unfall kommt (Wahrscheinlichkeit null). Es bleibt unberücksichtigt, dass während der Zeit des Bremsens von Zug 2 sich Zug 1 ggf. weiterbewegt. Dies ist eine Annahme zur sicheren Seite.

Unter Annahme der oben ausgeführten Randbedingungen kann eine Übertragung des Bremswegs in eine Wahrscheinlichkeit erfolgen. Ein linearer Ansatz ist jedoch nicht zielführend. Es verbleibt bei jedem Bremsvorgang eine Restwahrscheinlichkeit, dass der Bremsweg, obwohl rechnerisch ausreichend, nicht zur Vermeidung des Unfalls reicht. Je länger der berechnete Bremsweg ist, desto größer ist die verbleibende Restzusammenstoßwahrscheinlichkeit. Ein linearer Ansatz zur Berechnung der Zusammenstoßwahrscheinlichkeit trägt dem jedoch nicht Rechnung. Daher wird ein quadratischer Ansatz verfolgt, bei dem das Quadrat der Zusammenstoßwahrscheinlichkeit in die Berechnung der Unfallwahrscheinlichkeit eingeht (Bild 5.17).

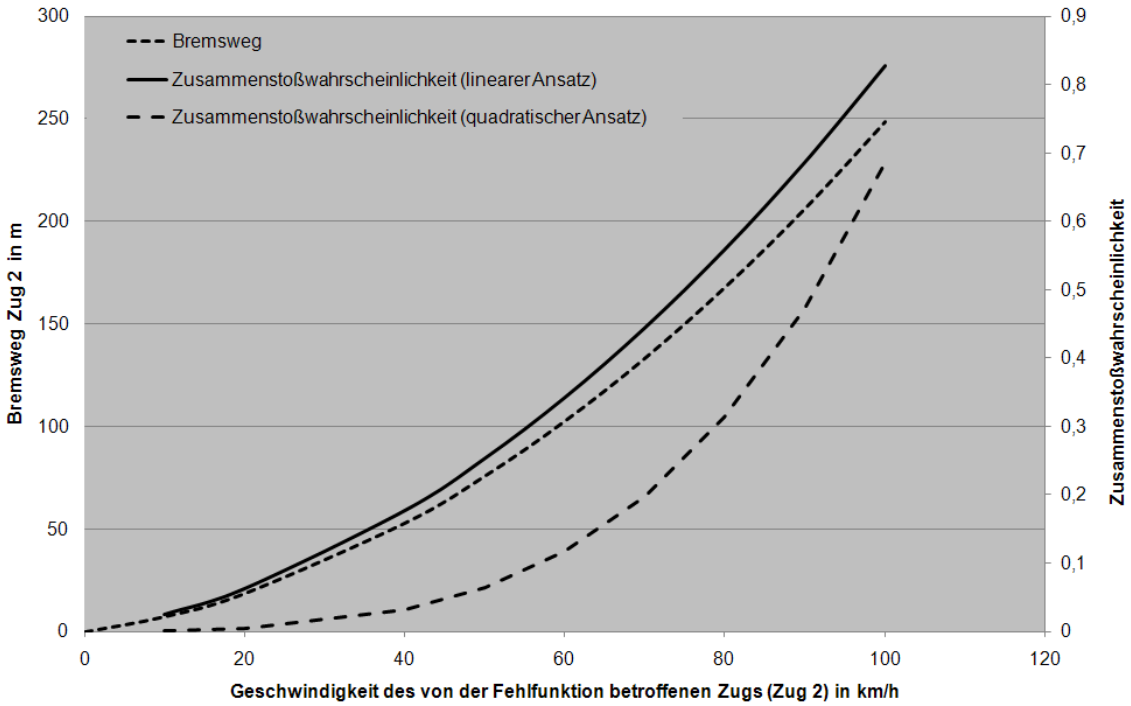

Bild 5.17: Darstellung der Auswirkungen eines quadratischen Ansatzes zur Ermittlung der Unfallwahrscheinlichkeit

Die ermittelte Zusammenstoßwahrscheinlichkeit muss kombiniert werden mit der Konfliktwahrscheinlichkeit. Diese betrachtet, ob es aufgrund des Verhältnisses der Geschwindigkeiten von Zug 1 und Zug 2 überhaupt zu einem Unfall bzw. Beinah-Unfall kommen kann. Es sind zwei Szenarien für die Grenzwertbetrachtung zu analysieren:

- Zug 1 fährt mit Streckengeschwindigkeit: Es kann nicht zu einem Unfall kommen, da beide Züge gleich schnell fahren und so keine Annäherung stattfindet. Die Konfliktwahrscheinlichkeit beträgt null.

- Zug 1 steht im betrachteten Block: Es findet sicher eine Annährung des Zuges 2 an Zug 1 statt. Die Konfliktwahrscheinlichkeit beträgt eins.

Basierend auf den getroffenen Annahmen kann durch Interpolation der Zwischenwerte zwischen dem günstigsten bzw. ungünstigsten Fall die Konfliktwahrscheinlichkeit berechnet werden (Bild 5.18).

Für ausgewählte, maßgebliche Geschwindigkeiten von Zug 1 wird das Produkt aus (konstanter) geschwindigkeitsabhängiger Konfliktwahrscheinlichkeit und variabler Zusammenstoßwahrscheinlichkeit gebildet. Die Berechnung der Unfallwahrscheinlichkeit ist in Bild 5.19 dargestellt. Bild 5.20 zeigt das resultierende Diagramm zur Ermittlung der Unfallwahrscheinlichkeitsklasse bei Verletzungen des Folgefahrschutzes.

Die Unfallwahrscheinlichkeit, dass es bei Verletzungen des Gegenfahrschutzes zu einem Unfall kommt, kann in Anlehnung an obiges Vorgehen zur Ermittlung der Zusammenstoßwahrscheinlichkeit ermittelt werden. Die Konfliktwahrscheinlichkeit beträgt eins. Der von der

Geschwindigkeit Zug 2 [km/h]	Geschwindigkeit Zug 1 [km/h]	Konfliktwahrscheinlichkeit (interpoliert)
120	120	0,00
120	110	8,33
120	100	16,67
120	90	25,00
120	80	33,33
120	70	41,67
120	60	50,00
120	50	58,33
120	40	66,67
120	30	75,00
120	20	83,33
120	10	91,67
120	0	100,00

Bild 5.18: Ermittlung der Konfliktwahrscheinlichkeit bei Verletzungen des Folgefahrschutzes

		Zug 1 steht	Zug 1 fährt mit 50 km/h	Zug 1 fährt mit 80 km/h	Zug 1 fährt mit 110 km/h
Geschwindigkeit Zug 2	Bremsweg	Konfliktwahrscheinlichkeit 100 Prozent	Konfliktwahrscheinlichkeit 58 Prozent	Konfliktwahrscheinlichkeit 33 Prozent	Konfliktwahrscheinlichkeit 8 Prozent
0	0,00	0,00	0,00	0,00	0,00
10	7,48	0,02	0,01	0,01	0,00
20	18,83	0,06	0,04	0,02	0,01
40	53,09	0,18	0,10	0,06	0,01
50	76,00	0,25	0,15	0,08	0,02
60	102,78	0,34	0,20	0,11	0,03
70	133,41	0,44	0,26	0,15	0,04
80	167,90	0,56	0,33	0,19	0,05
90	206,25	0,69	0,40	0,23	0,06
100	248,46	0,83	0,48	0,28	0,07
120	344,44	1,00	0,58	0,33	0,08

Bild 5.19: Ermittlung der Unfallwahrscheinlichkeit bei Verletzungen des Folgefahrschutzes

Fehlfunktion betroffene Zug wird in Übereinstimmung mit der obigen Folgefahrschutzbetrachtung als Zug 2 bezeichnet (Bild 5.21). Die Wahrscheinlichkeit, dass es zu einem Unfall kommt, wenn zwei Fahrzeuge aufeinander zu fahren bzw. ein Fahrzeug sich auf einen stehenden Zug zu bewegt, ist maßgeblich abhängig von der Sichtentfernung, der Reaktionszeit t_R und der Geschwindigkeit des Fahrzeugs v_0. Es sind die während Reaktions- und Bremszeit zurückgelegten Wege dem Abstand zum anderen Fahrzeug gegenüberzustellen. Es wird von einer Sichtentfernung von 300 Metern ausgegangen und es werden durchschnittliche (typische) Sichtbedingungen angenommen. Es wird von einer maximalen Bremsverzögerung a_{beschl} von 2 $\frac{m}{s^2}$ sowie einer Reaktionszeit von 2 Sekunden ausgegangen. Die während der Reaktionszeit zurückgelegte Strecke s_R berechnet sich zu $s_R = v_0 * t_R$. Die während des Bremsens zurückgelegte Strecke s_B berechnet sich zu $s_B = 0,5 * v_0^2 * a_{beschl}^{-1}$. Die Formeln werden für beide Fahrzeuge angesetzt. Es kommt zu einem Zusammenstoß, wenn die Summe aus Brems- und Reaktionsstrecke der beiden Fahrzeuge größer als die zur Verfügung stehende Sichtstrecke von 300 Metern ist. Zur Berechnung der Wahrscheinlichkeit wird angesetzt, dass bei einem negativen ermittelten Abstand es sicher zu einem Unfall kommt (Unfallwahrscheinlichkeit eins) und bei einem Abstand von 300 Metern (beide Fahrzeuge stehen sich gegenüber, aber fahren nicht aufeinander zu) es sicher nicht zu einem Unfall kommt (Unfallwahrscheinlichkeit null). In Übereinstimmung mit der Argumentation bei der Berechnung der Zusammenstoßwahrscheinlichkeit wird kein linearer, sondern ein quadratischer Ansatz zur Berechnung der Unfallwahrscheinlichkeit ver-

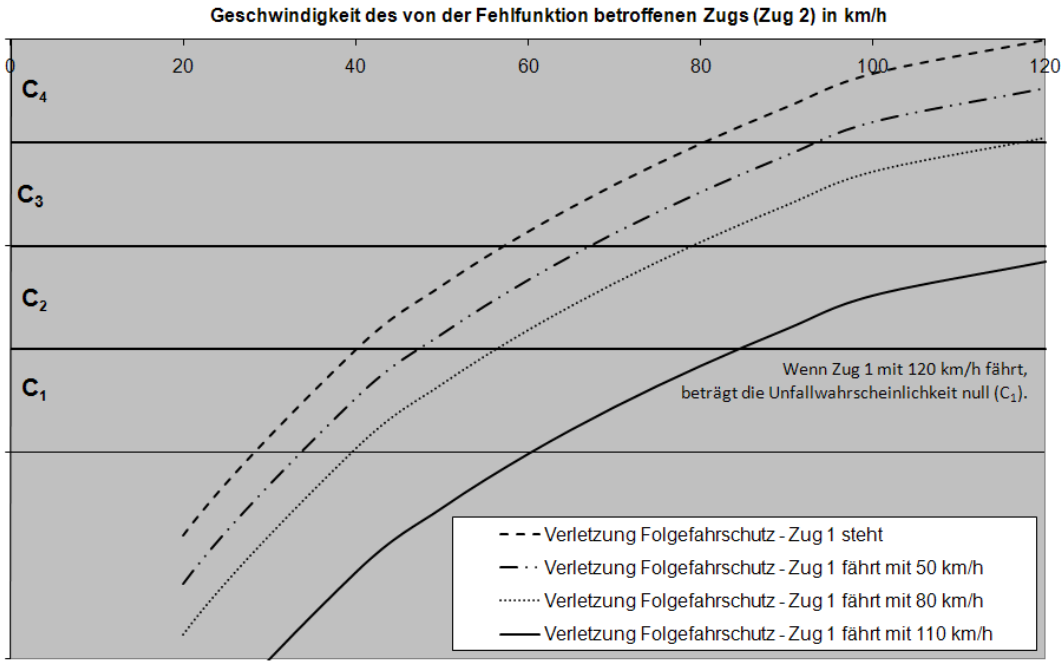

Bild 5.20: Diagramm zur Ermittlung der Unfallwahrscheinlichkeitsklasse bei Verletzungen des Folgefahrschutzes

Bild 5.21: Begriffsvereinbarung für Verletzungen des Gegenfahrschutzes

folgt. Die Berechnung kann Bild 5.22 entnommen werden. Das resultierende Diagramm der Unfallwahrscheinlichkeit bei Verletzungen des Gegenfahrschutzes ist in Bild 5.23 dargestellt.

		Verletzung des Gegenfahrschutz - Zusammenstoß			
		v2= 0km/h	v2= 50km/h	v2= 80km/h	v2= 120km/h
Geschwindigkeit Fahrzeug 2 in km/h	Bremsweg in [m]	0,00	76,00	167,90	344,44
10	7,48	0,00	0,08	0,34	1,00
20	18,83	0,00	0,10	0,39	1,00
40	53,09	0,03	0,19	0,54	1,00
60	102,78	0,12	0,36	0,81	1,00
70	133,41	0,20	0,49	1,00	1,00
80	167,90	0,31	0,66	1,00	1,00
90	206,25	0,47	0,89	1,00	1,00
100	248,46	0,69	1,00	1,00	1,00
120	344,44	1,00	1,00	1,00	1,00

Bild 5.22: Ermittlung der Unfallwahrscheinlichkeit bei Verletzungen des Gegenfahrschutzes

Die beiden anderen, oben betrachteten Fälle (fehlender Flankenschutz bzw. fehlender Schutz vor einem Hindernis im Gleis) entsprechen bezüglich der anzunehmenden Unfallwahrscheinlichkeit dem Fall des fehlenden Gegenfahrschutzes, wenn Zug 1 steht.

5.11 Parameter Aussetzungszeit und Gefährdungsdauer *DE*

Die Parameter Aussetzungszeit und Gefährdungsdauer gehen als Summe in die Risikoberechnung ein. Da der Risikograph nur multiplikativ verknüpfte Parameter abbilden kann, müssen beide Einflussgrößen in einem Parameter abgebildet werden. Im Folgenden werden zunächst beide Einflussgrößen analysiert, bevor ein Vorgehen zum Ableiten eines gemeinsamen Parameters *DE* vorgestellt wird.

Der Wert für die Aussetzungszeit E beschreibt, welche Zeit das Individuum bzw. das betrachtete Kollektiv der Gefährdung ausgesetzt ist (nach Braband (2005)).

Die Aussetzungszeit kann ermittelt werden, indem das Produkt gebildet wird aus Anzahl der Überfahrungen bzw. Inanspruchnahmen des Elements und der jeweiligen Dauer. Eine Abschätzung zur sicheren Seite ist es, E mit eins anzunehmen, d.h. davon auszugehen, dass der betrachtete Zug während der gesamten Betriebsstunde dem Element ausgesetzt ist. Diese Abschätzung führt jedoch zu konservativen Ergebnissen. Im Rahmen der Risikographerstellung wird das folgende Vorgehen verfolgt:

Jedes Element kann betrieblich einem Fahrstraßenabschnitt zugeordnet werden. Es wird davon ausgegangen, dass zu jedem Zeitpunkt während der Belegung des Abschnitts eine Anforderung an die Komponente kommen kann. Die Belegungszeit eines Abschnitts setzt sich aus verschiedenen Bestandteilen zusammen. Jedem dieser Bestandteile kann eine Wegstrecke bzw. eine Zeit zugeordnet werden. Folgende Bestandteile sind für die Fahrt auf freier Strecke zu berücksichtigen. Die Zahlenwerte wurden Pachl u. Milius (2009) entnommen.

- Fahrstraßenbildezeit (5 Sekunden)
- Sichtstrecke (300 m)
- Annäherungsfahrzeit, vom Vorsignal zum Hauptsignal (1000 m)
- Blockfahrzeit (anzunehmende Blocklänge ist abhängig vom betrachteten Szenario)

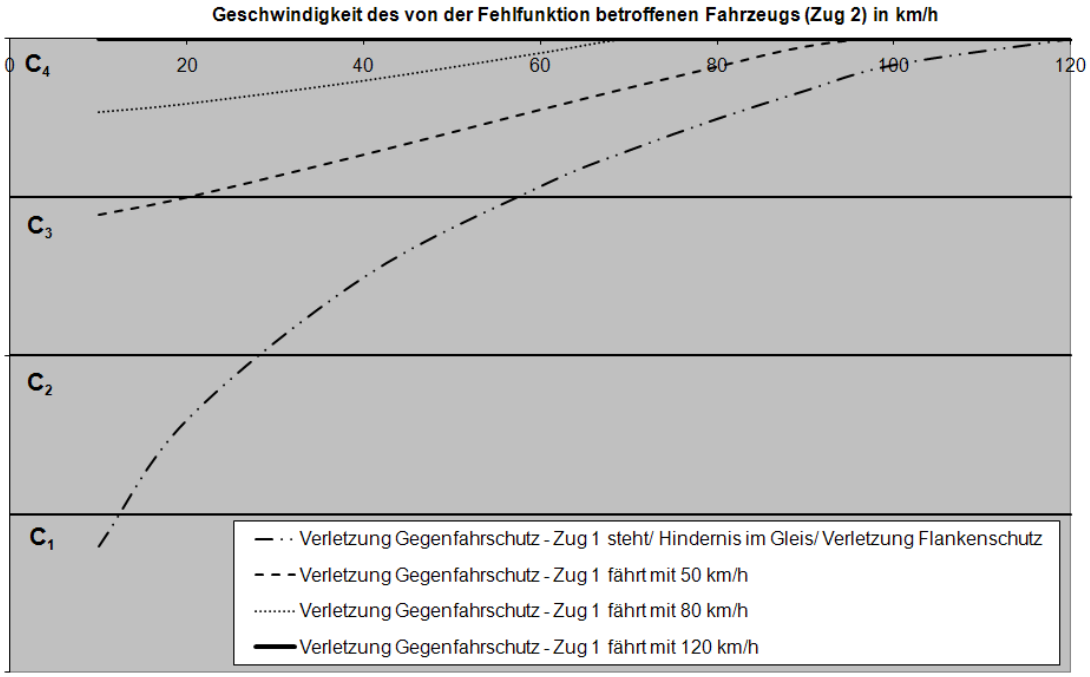

Bild 5.23: Diagramm zur Ermittlung der Unfallwahrscheinlichkeitsklasse bei Verletzungen des Gegenfahrschutzes

- Räumfahrzeit für die angenommene Zuglänge von 300 m und den Durchrutschweg von 50 m
- Fahrstraßenauflösezeit (3 Sekunden)

Die Zahl der in einer Stunde eine Komponente überfahrenden Züge und deren Verteilung innerhalb der Stunde ist abhängig vom Betriebsprogramm. Zur Ermittlung der Gesamtaussetzungszeit wird das in Abschnitt 5.8 abgeleitete Szenario zu Grunde gelegt. Es wird davon ausgegangen, dass der Zug eine Komponente so oft überfährt, wie dies in der Realität innerhalb der betrachteten Stunde der Fall ist.

Für alle Gefährdungen, die zu einem Zusammenstoß eines Zuges mit einem zweiten Zug führen, muss bei der Ergebnisermittlung berücksichtigt werden, dass ein zweiter, potentiell betroffener Zug sich in der Nähe befindet. Ein Unfall kann nur auftreten, wenn sich die Züge im gleichen oder in benachbarten Abschnitten befinden. Es ist nicht möglich, diesen Einfluss des Betriebsprogramms im Rahmen der Reduktionsfaktoren zu berücksichtigen, da es sich nicht um eine Reduktion der Unfallwahrscheinlichkeit handelt, sondern vielmehr um eine Auswirkung auf die Auftretenshäufigkeit der Gefährdung. Die Wirkung des Betriebsprogramms liegt im Ablauf von der Funktion zum Unfall noch vor dem Eintreten der Gefährdung. Der Einfluss des Betriebsprogramms muss im Rahmen der Aussetzungszeit berücksichtigt werden.

Die obigen Erörterungen gelten für die freie Strecke. Es ist zu diskutieren, welche Anpassungen notwendig sind, wenn Fehlfunktionen im Bahnhof analysiert werden sollen. Die Infrastruktur in einem Bahnhof kann sehr unterschiedlich sein. Auch haben neben dem Betriebsprogramm der betrachteten Strecke die Funktion des Bahnhofs im Netz und die Betriebsprogramme anschließender Strecken Auswirkungen auf die Aussetzungszeit im Bahnhof.

Funktionen werden ggf. deutlich häufiger in Anspruch genommen, als dies auf der freien Strecke der Fall ist. Darüber hinaus spielen besondere betriebliche Aufgaben wie z.B. das Rangieren und die damit verbundene erhöhte Wahrscheinlichkeit für z.B. ein Hindernis im Gleis eine Rolle. Die Vielzahl dieser Einflüsse kann nicht im Risikograph abgebildet werden. Daher ist es notwendig, eine qualitative Argumentation für ein im Risikographen umsetzbares Vorgehen zu finden. Grundsätzlich kann davon ausgegangen werden, dass die Aussetzungszeit im Bahnhof deutlich größer anzunehmen ist, als auf der freien Strecke. Die Abschätzung zur sicheren Seite, d.h. die Annahme, dass E zu eins wird, führt zu konservativen Ergebnissen. Es wird festgelegt, dass, wird ein Szenario im Bahnhof als relevant betrachtet, der in Bild 5.25 angegebene Zahlenwert zu verdoppeln ist. Da die Aussetzungszeit maximal gleich der Betrachtungszeit werden kann, ist bei berechneten Werten größer als eins der Wert eins anzunehmen.

Die Berechnung der Belegungszeiten und die daraus resultierenden Werte für den Parameter E kann den Abbildungen 5.24 und 5.25 entnommen werden.

Für die Gefährdungsdauer D kann kein oberer Grenzwert als Abschätzung zur sicheren Seite angenommen werden, da theoretisch die Gefährdungsdauer beliebig groß werden kann.

Aufgrund des im Risikomodell vorgesehenen Zusammenhangs von E und D sind die beiden Größen E und D in einem Parameter DE abzubilden. Zwischen den Parameterklassengrenzen kann wahlweise der Faktor 10 (in Übereinstimmung mit dem Faktor zwischen den Ergebnisklassen) oder der Faktor $\sqrt{10}$ (in Übereinstimmung mit dem Faktor zwischen den Schadensparameterklassengrenzen) liegen. Der Grundwert der Ableitung wird basierend auf folgendes Szenario ermittelt: Es wird eine Gefährdung betrachtet, die auf einer hochbelasteten Strecke auftritt (E nahe eins) und nur wenige Minuten besteht. Es wird abgeschätzt, dass dieses Szenario zu einer Parameterklassengrenze mit dem Wert 1 führt. Die weiteren Klassengrenzen ergeben sich durch Anwendung des entsprechenden Faktors. Wird der Faktor $\sqrt{10}$ angenommen, so ergeben sich die weiteren Klassengrenzwerte zu 0,31 und 0,1 bzw. 3,16, 10, 31,6 und 100.

Der untere Grenzwert wird durch das Szenario kurze Aufenthaltsdauer und kurze Gefährdungsdauer ermittelt. Laut Bild 5.25 ist der kleinste Wert für E 0,033. Wenn als untere Grenze für DE 0,1 gewählt wird, dürfte D maximal den Wert 0,067 annehmen. Dies entspricht einer Gefährdungsdauer von vier Minuten. Es erscheint nicht möglich, dass eine Gefährdungsdauer zuverlässig derart klein abgeschätzt wird. Auch wird davon ausgegangen, dass Gefährdungen, die zu einer Summe aus D und E von kleiner 0,1 führen, sehr selten sind. Daher wird als Wert für den Parameter DE minimal 0,31 (bei Faktor $\sqrt{10}$) oder 1 (bei Faktor 10) gewählt.

Die Aufenthaltsdauer E spielt für den oberen Klassengrenzwert keine Rolle, da E im Verhältnis zu D sehr klein ist. Wird der Wert 31,6 als oberer Grenzwert gewählt, so muss der Faktor $\sqrt{10}$ beibehalten werden, und es ergeben sich fünf Klassen. Wird stattdessen als oberer Grenzwert der Wert 100 gewählt, so ergeben sich bei Anwendung des Faktors $\sqrt{10}$ sechs Klassen, bzw. bei Anwendung des Faktors 10 drei Klassen. Unter Berücksichtigung der Tatsache, dass beide Werte E und D Schätzwerte sind und daher von einer Ungenauigkeit ausgegangen werden muss und der Tatsache, dass fünf bzw. sechs Klassen für einen Risikographen zu zu detaillierten Ergebnissen führen, wird der Faktor 10 für die Ableitung der Parameterklassengrenzen herangezogen.

Die festgelegten Parameterklassengrenzen können Tabelle 5.6 entnommen werden. Die Werte gelten für die Summe aus D und E. Unter Annahmen für E können die Werte für D ermittelt werden. Das Diagramm zur Ermittlung des Parameters DE kann Abbildung 5.26 entnommen werden.

Für den Bereich des Bahnhofs wird davon ausgegangen, dass eine Fehlfunktion unter an-

		Geschwindigkeit 50 km/h			Geschwindigkeit 80 km/h			Geschwindigkeit 100 km/h			Geschwindigkeit 120 km/h		
	Weg [m]	Zeit [s]											
Fahrstraßenbildezeit		5	5	5	5	5	5	5	5	5	5	5	5
Sichtzeit Vorsignal	300	21,6	21,6	21,6	13,5	13,5	13,5	10,8	10,8	10,8	9	9	9
Annäherungsfahrzeit	1000	72	72	72	45	45	45	36	36	36	30	30	30
Blockfahrzeit	2000	144			90			72			60		
	5000		360			225			180			150	
	10000			720			450			360			300
Räumfahrzeit D-Weg	50	3,6	3,6	3,6	2,25	2,25	2,25	1,8	1,8	1,8	1,5	1,5	1,5
Räumfahrzeit Zuglänge	300	21,6	21,6	21,6	13,5	13,5	13,5	10,8	10,8	10,8	9	9	9
Fahrstraßenauflösezeit		3	3	3	3	3	3	3	3	3	3	3	3
Belegungszeit des Blocks		**270,8**	**486,8**	**846,8**	**172,25**	**307,25**	**532,25**	**139,4**	**247,4**	**427,4**	**117,5**	**207,5**	**357,5**

Bild 5.24: Berechnung der Belegungszeit

	Anzahl Züge pro Stunde					
	1	2	3	4	5	6
Wert für E bei v = 50 km/h						
Blocklänge 2000 m	0,075	0,150	0,226	0,301	0,376	0,451
Blocklänge 5000 m	0,135	0,270	0,406	0,541	0,676	0,811
Blocklänge 10000 m	0,235	0,470	0,706	0,941	1,000	1,000
Wert für E bei v = 80 km/h						
Blocklänge 2000 m	0,048	0,096	0,144	0,191	0,239	0,287
Blocklänge 5000 m	0,085	0,171	0,256	0,341	0,427	0,512
Blocklänge 10000 m	0,148	0,296	0,444	0,591	0,739	0,887
Wert für E bei v = 100 km/h						
Blocklänge 2000 m	0,039	0,077	0,116	0,155	0,194	0,232
Blocklänge 5000 m	0,069	0,137	0,206	0,275	0,344	0,412
Blocklänge 10000 m	0,119	0,237	0,356	0,475	0,594	0,712
Wert für E bei v = 120 km/h						
Blocklänge 2000 m	0,033	0,065	0,098	0,131	0,163	0,196
Blocklänge 5000 m	0,058	0,115	0,173	0,231	0,288	0,346
Blocklänge 10000 m	0,099	0,199	0,298	0,397	0,497	0,596

Bild 5.25: Parameter Aussetzungszeit E in der Einheit Stunde [h] (bei Betrachtungen im Bahnhof ist der Tabellenwert zu verdoppeln; bei Werten größer 1 ist der Wert 1 anzunehmen)

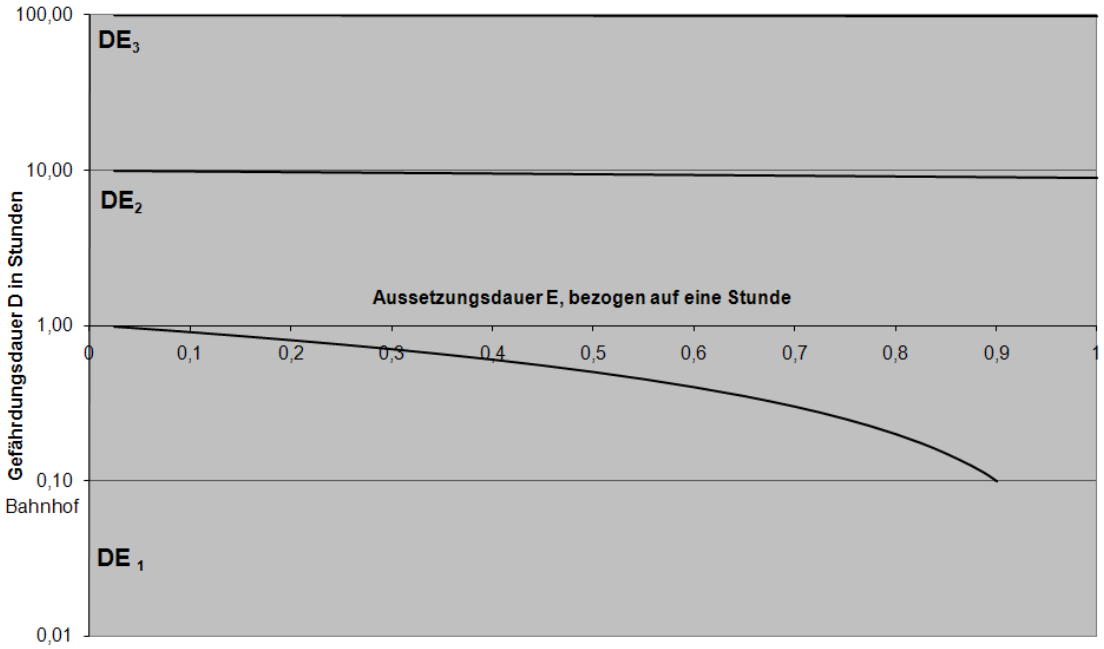

Bild 5.26: Diagramm zur Ermittlung des Parameters Aussetzungszeit/Gefährdungsdauer DE

Klassengrenzen/Summe E und D	1	10	100
Bezeichnung	DE_1	DE_2	DE_3

Tabelle 5.6: Parameter Aussetzungsdauer/Gefährdungsdauer

derem aufgrund der im Vergleich zur freien Strecke höheren Betriebsdichte und der größeren Wahrscheinlichkeit, dass sich Mitarbeiter eines EVU oder EIU vor Ort befinden und zur Aufdeckung beitragen können, mit D gleich 0,1 abgeschätzt werden kann. Bei Gefährdungsbestehenszeiten, die über 100 Stunden hinausgehen, ist die Analyse der Gefährdung nur mit Vorsicht und ggf. nach Rücksprache mit der zuständigen Genehmigungsstelle anwendbar.

Die Bandbreite der Werte für *DE* ist groß. Der Abstand zwischen der niedrigsten und der höchsten Klassengrenze beträgt ungefähr Faktor 100. Daher erscheint es nicht sinnvoll, wenn *DE* als Konstante in den Risikographen eingeht. Sollte sich zeigen, dass stets die gleiche Parameterklasse für *DE* gewählt wird, kann eine entsprechende Vereinfachung des Risikographen erfolgen.

5.12 Der menschliche Fehler bei latenten Gefährdungen

Sowohl latente als auch direkte Gefährdungen können mit dem Risikographen analysiert werden. Das für direkte Gefährdungen abgeleitete Ergebnis kann direkt angewendet werden. Es sind keine weiteren betrieblichen Einflüsse zu berücksichtigen.

Das für latente Gefährdungen abgeleitet Ergebnis kann nicht direkt übertragen werden. Für die Fehlerraten bzw. die Fehlerwahrscheinlichkeit von Menschen gibt es unterschiedliche Ansätze (z.B. Tabelle 5.8 aus VDI 4006, Blatt 2 (2003), Hinzen (1993)).

Menschl. Verhaltens-ebene	günstige Umweltbedingungen			ungünstige Umweltbedingungen		
	Streß durch Unterfor-derung	optimales Streß-niveau	Streß durch Überfor-derung	Streß durch Unterfor-derung	optimales Streß-niveau	Streß durch Über-forderung
fertigkeits-basierend	$2 \cdot 10^{-3}$	$1 \cdot 10^{-3}$	$2 \cdot 10^{-3}$	$1 \cdot 10^{-2}$	$5 \cdot 10^{-3}$	$1 \cdot 10^{-2}$
regel-basierend	$2 \cdot 10^{-2}$	$1 \cdot 10^{-2}$	$2 \cdot 10^{-2}$	$1 \cdot 10^{-1}$	$5 \cdot 10^{-2}$	$1 \cdot 10^{-1}$
wissens-basierend	$2 \cdot 10^{-1}$	$1 \cdot 10^{-1}$	$5 \cdot 10^{-1}$	1	$5 \cdot 10^{-1}$	1

Tabelle 5.7: Wahrscheinlichkeit für menschliche Fehler nach Hinzen (1993)

In bisherigen Risikoanalysen im Eisenbahnwesen wurde im Allgemeinen die Fehlerwahrscheinlichkeit nach Hinzen berücksichtigt. In seiner Dissertation von 1993 hat Hinzen zunächst die unterschiedlichen Einflüssen auf das Verhalten des Menschen analysiert und ein qualitatives Modell menschlichen Verhaltens abgeleitet. Eine Auswertung der Aussagen zur menschlichen Fehlerwahrscheinlichkeit in der eisenbahntechnischen Fachliteratur wird von ihm als nicht geeignet für eine weitere Verwendung eingeschätzt, da die Aussagen lediglich auf Annahmen bzw. nicht geeigneten Analysen beruhen. Er führt eine Auswertung der europäischen und im Besonderen amerikanischen Literatur aus der Sicherheitswissenschaft (Reaktorsicherheit) der achtziger Jahre durch. Durch Abbildung der dort angegebenen Fehlerwahrscheinlichkeiten auf das erstellte qualitative Modell kommt er zu der Zusammenstellung von Fehlerwahrscheinlichkeiten wie in Tabelle 5.7 angegeben. Auch wenn die abgeleiteten Werte vielfach eingesetzt werden, so sollte deren Verwendung doch kritisch gesehen werden. Die Ableitung der Werte beruht nicht auf Analysen aus dem Eisenbahnwesen, sondern der Reaktorsicherheit. Es ist davon

auszugehen, dass ergonomisch relevante Unterschiede in der Verarbeitung der anfallenden Aufgaben bestehen. Hinzu kommt, dass es sich um ältere Studien handelt und sich die ergonomischen Analysemethoden weiterentwickelt haben. Auch ist zu berücksichtigen, dass an heutigen Arbeitsplätzen eine Verschiebung von vorwiegend körperlich auszuführenden Aufgaben hin zu Tätigkeiten am Rechner erfolgt. Es steht zu erwarten, dass diese Schwerpunktverschiebung Auswirkungen auf die Fehlerwahrscheinlichkeiten hat. Daher erscheint es sinnvoll, die aktuelle Literatur nach weiteren quantitativen Angaben zur Fehlerwahrscheinlichkeit auszuwerten.

Die Richtlinie VDI 4006, Blatt 2 (2003) stellt die Methoden zur quantitativen Bewertung menschlichen Handelns im technischen Umfeld vor und beschreibt die Analyse der notwendigen, grundlegenden Arbeitsschritte. Es werden Aussagen zur menschlichen Fehlerwahrscheinlichkeit getroffen. Es wird ausgesagt, dass die menschliche Fehlerwahrscheinlichkeit basierend auf aufgabenspezifische Fehlerstatistiken abgeleitet werden sollte. Liegt eine solche Statistik nicht vor, kann auf ein prädikatives Vorgehen zurückgegriffen werden. Die in Tabelle 5.8 gegebenen Zahlenwerte sind VDI 4006, Blatt 2 (2003) entnommen. Sie geben einen allgemeinen Überblick über Größenordnungen von Wahrscheinlichkeiten für menschliche Fehler bei unterschiedlichen Aufgaben in Abhängigkeiten von den situativen Anforderungen und der kognitiven Belastung. Die Werte können laut Straeter (2009) für Screening-Analysen, d.h. überschlägige Bewertungen von menschlichen Fehlerwahrscheinlichkeiten herangezogen werden. Es kann daher davon ausgegangen werden, dass es sich um konservative Abschätzungen handelt. Um detaillierte Aussagen treffen zu können, sind detaillierte Aufgabenanalysen und die Anwendung von ausgewählten Bewertungsmethoden notwendig. Die Richtlinie wurde im entsprechenden VDI-Arbeitskreis entwickelt und abgestimmt. Es kann davon ausgegangen werden, dass sie den Stand der Technik darstellt.

In Bild 5.27 sind die Zahlenwerte nach Hinzen (1993) und VDI 4006, Blatt 2 (2003) gegenübergestellt. Der Vergleich macht deutlich, dass die Zahlenwerte in der gleichen Größenordnung liegen. Es wird aufgrund der größeren Aktualität der Auswertung bzw. Veröffentlichung für die Arbeit auf die in VDI 4006, Blatt 2 (2003) veröffentlichten Zahlenwerte zurückgegriffen.

Die in VDI 4006, Blatt 2 (2003) vorgenommene Darstellung der menschlichen Zuverlässigkeit in Klassen ist gut geeignet für die Einbindung im Risikographen. Es erscheint sinnvoll, nur die drei Klassen MF_1, MF_2 und MF_3 zu unterscheiden. Die beiden Klassen MF_4 und MF_5 werden nicht berücksichtigt, da die beschriebenen Situationen im Allgemeinen im Eisenbahnbetrieb nicht vorkommen. Auch ist zu diskutieren, ob eine Fehlerwahrscheinlichkeit von eins für eine Quantifizierung im Rahmen einer Risikoabschätzung sinnvoll ist. Der Parameter wird als MF bezeichnet.

Werden eine Rate und eine Wahrscheinlichkeit per UND-Verknüpfung miteinander verbunden, so ist das Ergebnis die Rate, mit der ein Zusammentreffen beider Ereignisse auftritt. Unter der Annahme der Unabhängigkeit der Ereignisse ist die Rate das Produkt aus Ausfallrate der technischen Komponente und Wahrscheinlichkeit der menschlichen Fehlhandlung. Um die zulässige Ausfallrate für die Komponente zu ermitteln, ist die Gefährdungsrate des Gesamtsystems durch die menschliche Fehlerwahrscheinlichkeit zu dividieren. Die zu berücksichtigenden menschlichen Fehlerwahrscheinlichkeiten 0,1 für MF_3, 0,01 für MF_2 und 0,001 für MF_1 bedeuten eine Verschiebung der Ergebnisgefährdungsraten jeweils um eine, zwei oder drei Größenordnungen.

Der Parameter MF wird auf das ermittelte Ergebnis, d.h. auf die ermittelte, zulässige Gefährdungsrate angewendet.

Beschreibung		Wahrscheinlichkeiten
Einfache und häufig durchgeführte Aufgaben bei geringem Stress und genügend zur Verfügung stehender Zeit in gewohnten Situationen (z.B. ohne ablenkende oder störende zusätzliche Einflüsse, gute Rückmeldung)	MF_1	$1 \cdot 10^{-3}$
Komplexe und häufig durchgeführte Aufgaben in gewohnten Situationen mit geringem Stress und genügend zur Verfügung stehender Zeit, wobei eine gewisse Sorgfalt bei der Durchführung notwendig ist	MF_2	$1 \cdot 10^{-2}$
Komplexere und regelmäßig durchgeführte Aufgaben in ungewohnten Situationen (z.B. ablenkende oder störende Einflüsse, unzureichende Rückmeldung), bei hohem Stress oder geringer zur Verfügung stehender Zeit	MF_3	$1 \cdot 10^{-1}$
Komplexere und selten durchgeführte Aufgaben in ungewohnten Situationen (z.B. ablenkende oder störende Einflüsse, unzureichende Rückmeldung), bei hohem Stress oder geringer zur Verfügung stehender Zeit	MF_4	$3 \cdot 10^{-1}$
Hochkomplexe oder sehr selten durchgeführte Aufgaben in ungewohnten Situationen (z.B. ablenkende oder störende Einflüsse, unzureichende Rückmeldung), bei sehr hohem Stress oder geringer zur Verfügung stehender Zeit	MF_5	$1 \cdot 10^{-0}$

Tabelle 5.8: Wahrscheinlichkeit für menschliche Fehler nach VDI 4006, Blatt 2 (2003); Parameterbezeichnung im Rahmen der Arbeit

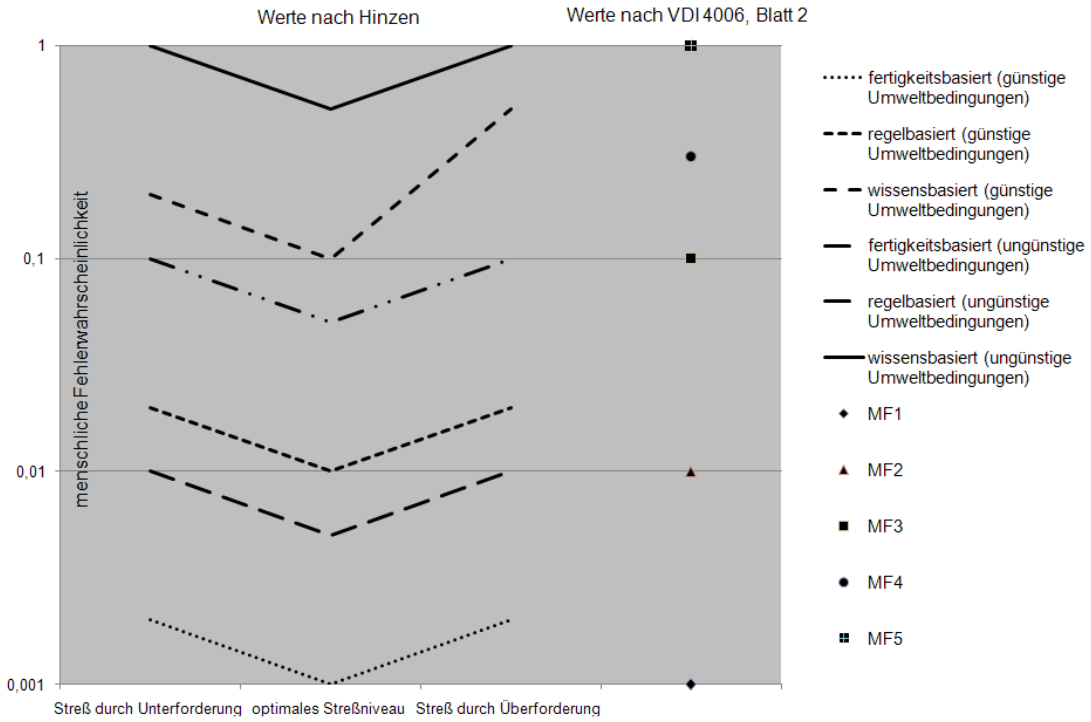

Bild 5.27: Vergleich der für menschliche Fehlerwahrscheinlichkeiten angenommenen Werte nach Hinzen (1993) und VDI 4006, Blatt 2 (2003)

5.13 Ableitung des Risikographen

In der Tabelle 5.9 sind die Parameter und ihre Klassen sowie die zugehörigen Rechenwerte zusammengestellt. Um den mathematischen Zusammenhang der Klassengrenzen zu verdeutlichen, erfolgt für die Parameter F und C zusätzlich die Darstellung mit Variablen.

Die Ergebnisableitung erfolgt durch Kalibrierung der Methode mit dem Kriterium RAC-TS auf Basis des Risikomodells. Es ist diejenige Parameterklassenkombination auszuwählen, die den in RAC-TS formulierten Bedingungen entspricht. Die gewählte Parameterkombination und der Benchmarkwert beschreiben einen Risikobereich, nicht einen expliziten Risikowert. Daher ist die rechnerische Kalibrierung mit Hilfe einzelner Klassengrenzwerte schwierig. Es wird vorgeschlagen, die Kalibrierung mittels einer Tabelle vorzunehmen.

Es erfolgt zunächst basierend auf den Aussagen in Verordnung EG Nr. 352/ (2009) die Wahl der zu RAC-TS zugehörigen Parameterklassenkombination. Es werden folgende Annahmen getroffen:

- *katastrophale Folgen*: Ereignisse mit mehr als fünf Opfern werden als katastrophal bezeichnet[6]; entsprechende Ereignisse sind in der Parameterklasse F_5 erfasst.
- *unmittelbare...Folgen*: Der Reduktionsfaktor C_4 erfüllt die Anforderungen.
- Verordnung EG Nr. 352/ (2009) macht keine Aussagen zur Aussetzungs- und Gefährdungsbestehenszeit. Es wird für die Kalibrierung davon ausgegangen, dass eine Gefähr-

[6]Die Eingruppierung ist weniger restriktiv als dies bei Anwendung von z.B. DIN EN 50126 (2000) der Fall wäre. Die Begründung für das gewählte Vorgehen entspricht den Aussagen in Abschnitt 5.9.6

Parameter	Klassen	Grenzen	oberer Grenzwert
Schaden in Opfer	F_1	0,158	f
	F_2	0,5	$\sqrt{10} \cdot f$
	F_3	1,58	$10 \cdot f$
	F_4	5	$\sqrt{10} \cdot 10 \cdot f$
	F_5	mehr als 5	
Unfallwahrscheinlichkeit in Prozent	C_1	3	c
	C_2	10	$\sqrt{10} \cdot c$
	C_3	30	$10 \cdot c$
	C_4	100	$\sqrt{10} \cdot 10 \cdot c$
Aussetzungsdauer/Gefährdungsdauer in Stunden	DE_1	1	
	DE_2	10	
	DE_3	100	
menschl. Fehlerwahrscheinlichkeit	MF_1	0,001	
	MF_2	0,01	
	MF_3	0,1	

Tabelle 5.9: Übersicht über die Parameter

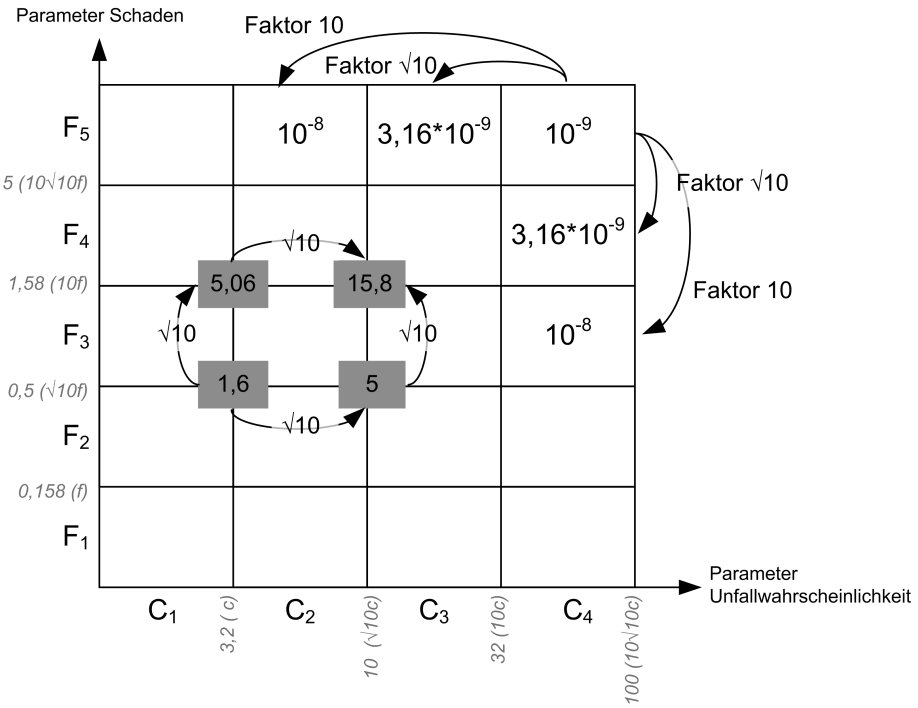

Bild 5.28: Schematisches Vorgehen zur Ableitung der zulässigen Gefährdungsraten

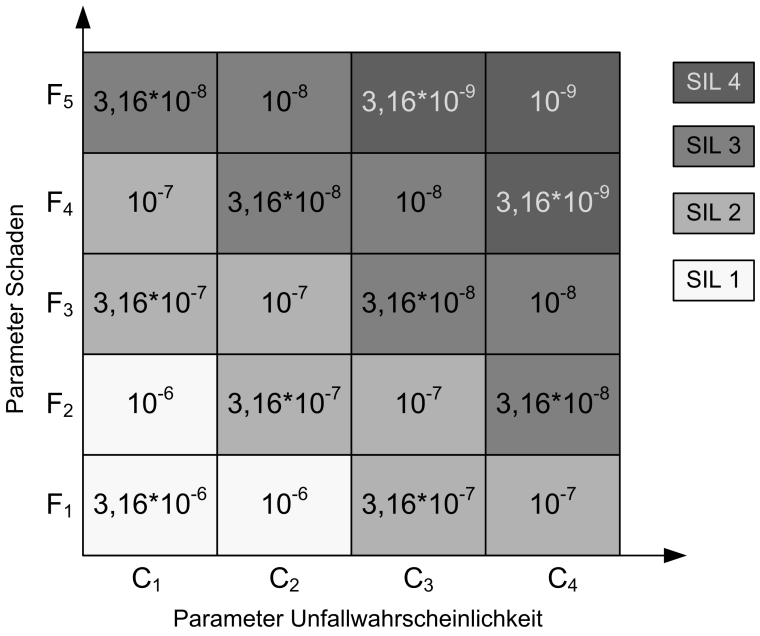

Bild 5.29: Ableitung der zulässigen Gefährdungsraten für die Parameterklassenkombinationen F_{1-5}, C_{1-4} und DE_2 in Gefährdungen je Stunde

dung, die unmittelbar zu katastrophalen Folgen führt, sich innerhalb einer Stunde offenbart. Dies ist keine Abschätzung zur sicheren Seite, aber aufgrund der Aussagen zur Gefährdungsdefinition, zum angenommenen Betrieb und zu den betrachteten Komponenten realistisch. Die Aussetzungszeit wird zu eins abgeschätzt. Es wird die Paramterklasse DE_2 gewählt.

Das schematische Vorgehen wird in Bild 5.28 illustriert. Der von RAC-TS beschriebene Risikobereich ist der Bereich in der oberen, rechten Ecke. Die Parameterklassengrenzen des Parameters Schaden F haben einen Abstand von $\sqrt{10}$. Gleiches gilt für die Parameterklassengrenzen des Paramters Unfallwahrscheinlichkeit C. Wird ausgehend vom Benchmarkszenario einer der beiden Parameter um eine Klasse reduziert, so ändert sich die zulässige Gefährdungsrate um den Faktor $\sqrt{10}$. Durch das beschriebene Vorgehen können alle Ergebnisklassen abgeleitet werden. Dass das Vorgehen in Übereinstimmung mit dem Risikomodell steht, kann ebenfalls gezeigt werden. Wird das Produkt der Parameterklassengrenzwerte von F und C an den Schnittpunkten im Diagramm gebildet, so beträgt der Abstand der Produkte jeweils $\sqrt{10}$. Bei konstantem Wert für den Parameter DE und konstantem Risiko schlägt sich dieser Abstand in der zulässigen Gefährdungsrate nieder.

Es werden in einem ersten Schritt die Ergebnisse für alle Szenarien F_{1-5}, C_{1-4} und DE_2 abgeleitet. Das Ergebnis kann Bild 5.29 entnommen werden.

In Übereinstimmung mit DIN EN 61508-5 (2002) werden die Klassen, die außerhalb des durch die Grenzen der SIL-Level beschriebenen Bereichs liegen mit a und b bezeichnet. In DIN EN 61508-5 (2002) wird der Bereich a definiert als *keine speziellen Sicherheitsanforderungen* und der Bereich b als *ein einzelnes E/E/PES ist nicht ausreichend*. Die Definition für a kann für den Beispielrisikographen übernommen werden. Da kein SIL abgeleitet werden kann, ist zu prüfen, ob Annahmen für diese Funktion in der Analyse getroffen wurden. Ist dies der

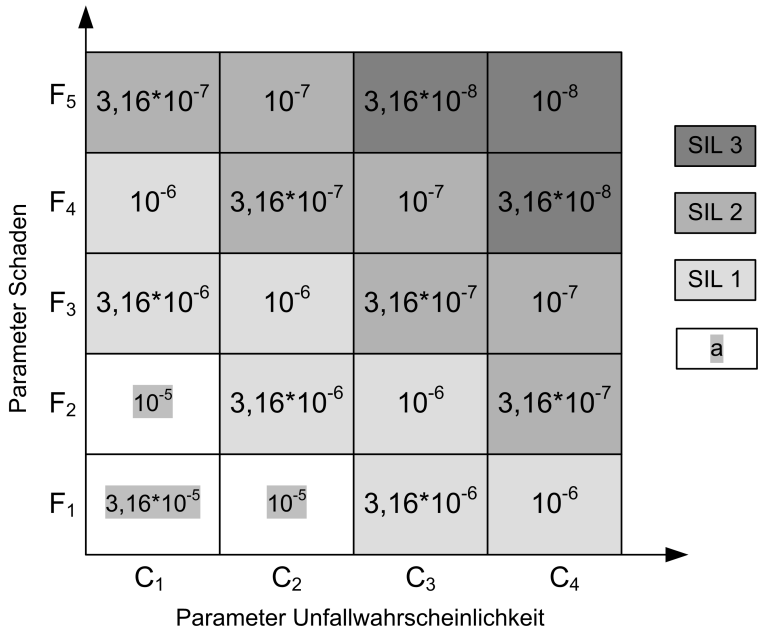

Bild 5.30: Ableitung der zulässigen Gefährdungsraten für die Parameterklassenkombinationen F_{1-5}, C_{1-4} und DE_1 Gefährdungen je Stunde

Fall, ist diese Funktion als Sicherheitsfunktion zu bezeichnen. Die Definition für den Bereich b ist aufgrund des veränderten Systemmodells nicht sinnvoll. Es wird definiert: Funktionen, für die als Ergebnis der Bereich b ermittelt wurde, sind durch den Konstrukteur gesondert zu analysieren. Es ist ein Vorschlag zu unterbreiten, wie die Sicherheitsanforderungen erreicht werden können, bzw. wie eine Reduktion der Sicherheitsanforderungen möglich ist.

Um Ergebnisse mit den Parametern DE_1 und DE_3 zu ermitteln, sind die Werte aus Bild 5.29 um jeweils den Faktor 10 zu verkleinern bzw. zu vergrößern (Bild 5.30 und 5.31).

Das Ergebnis kann zur Klassifizierung von direkten Gefährdungen angewendet werden. Der entsprechende Risikograph findet sich in Bild 5.32.

Um Ergebnisse für latente Gefährdungen zu erhalten, die nur bei Hinzukommen eines menschlichen Fehlers zu einem Unfallereignis führen, wurde der Parameter MF eingeführt. Die zu berücksichtigenden menschlichen Fehlerwahrscheinlichkeiten 0,1 für MF_3, 0,01 für MF_2 und 0,001 für MF_1 bedeuten eine Verschiebung der Ergebnisgefährdungsraten jeweils um eine, zwei oder drei Größenordnungen. Die Ergebnisse können nach Tabelle 5.10 ermittelt werden.

5.14 Diskussion des Beispielrisikographen

5.14.1 Randbedingungen

Der Risikograph kann angewendet werden für die Analyse von Funktionen des Reisezugverkehrs. Er kann nicht angewendet werden für beispielsweise güterzugspezifische Risiken oder Risiken in Rangieranlagen. Die Erstellung eines Risikographen für diese Bereiche erfordert z.B. die Anpassung der Schadensermittlung (z.B. Berücksichtigung von Sachschaden) und, als Basis für solche Anpassungen, die Festlegung von Meßgrößen zur Beurteilung von Schaden, der nicht in Personenschaden messbar ist und ggf. die Festlegung eines anderen Risikoak-

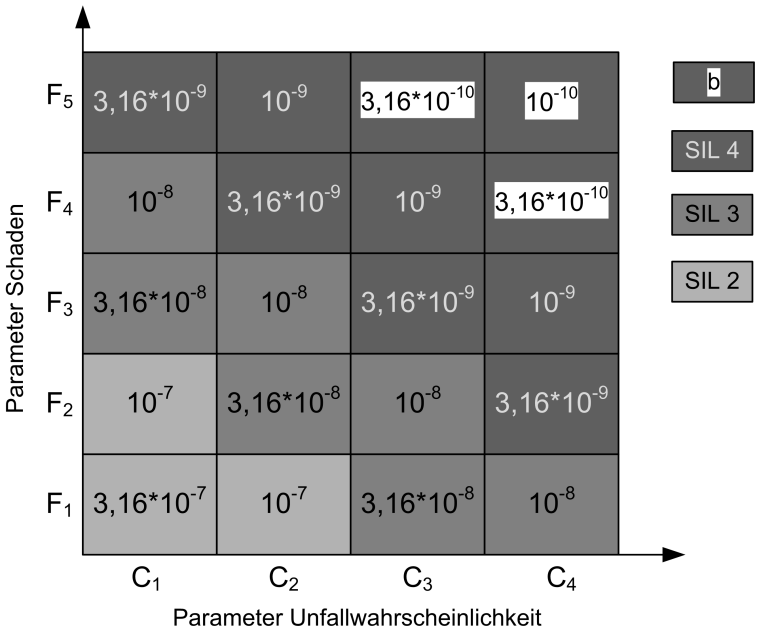

Bild 5.31: Ableitung der zulässigen Gefährdungsraten für die Parameterklassenkombinationen F_{1-5}, C_{1-4} und DE_3 Gefährdungen je Stunde

zeptanzkriteriums. Für Mischverkehrsstrecken wird davon ausgegangen, dass der Unfall von Personenzügen maßgeblich ist. Besonders zu beachten sind Züge, welche Gefahrgut transportieren, da bei einem Unfall dieser Züge eine große Zahl von Personen indirekt betroffen sein kann. Da nur wenige Daten zu den Auswirkungen von Gefahrguttransportunfällen vorliegen, muss, wenn der Unfall mit einem Gefahrguttransport als maßgeblich angenommen wird, dieser als Einzellfall betrachtet werden. Er kann nicht mit dem Risikographen analysiert werden.

Der Risikograph kann nicht für Bahnübergangsunfälle angewendet werden. Dieser Ausschluss wurde vorgenommen, da sich die Charakteristiken von Zusammenstoß und Entgleisung wesentlich vom Bahnübergangsunfall unterscheiden.

Die Definition der Analyseebene orientiert sich an der Realisierung. Durch die Verknüpfung von Funktion und Komponente entsteht automatisch eine Kopplung von Anforderung und Realisierung. Es können durch den Anwender unterschiedliche Funktionen und respektive unterschiedliche Gefährdungen abgeleitet werden. Es wird eine niedrige, realisierungsnahe Analyseebene gewählt. Eine system- bzw. realisierungsunabhängige Funktionsdefinition müsste auf einer höheren Ebene erfolgen.

5.14.2 Diskussion der Parameter und der Parameterermittlung

Im Unterschied zu anderen qualitativen und semi-qualitativen Verfahren erlaubt der entwickelte Risikograph eine weitgehend systematisierte Parameterklassenableitung. Der Anwender muss wenige betriebliche Daten abschätzen. Nach dieser Ermittlung der Eingangsgrößen sind die Freiheitsgrade des Anwenders, d.h. die Möglichkeiten zur Diskussion und zur Interpretation, gering. Durch die Kalibrierung des Schadensklassendiagramms anhand von statistisch erfassten Unfällen kann davon ausgegangen werden, dass Fahrzeug-/Wagentypen und deren Besetzungsgrad über die Unfälle gleichmäßig verteilt sind und damit implizit in die Parame-

Ausgangs- *HR*	MF_3 0,1	MF_2 0,01	MF_1 0,001
10^{-9}	10^{-8}	10^{-7}	10^{-6}
$3,16 \cdot 10^{-9}$	$3,16 \cdot 10^{-8}$	$3,16 \cdot 10^{-7}$	$3,16 \cdot 10^{-6}$
10^{-8}	10^{-7}	10^{-6}	10^{-5}
$3,16 \cdot 10^{-8}$	$3,16 \cdot 10^{-7}$	$3,16 \cdot 10^{-6}$	$3,16 \cdot 10^{-5}$
10^{-7}	10^{-6}	10^{-5}	10^{-4}
$3,16 \cdot 10^{-7}$	$3,16 \cdot 10^{-6}$	$3,16 \cdot 10^{-5}$	$3,16 \cdot 10^{-4}$
10^{-6}	10^{-5}	10^{-4}	10^{-3}
$3,16 \cdot 10^{-6}$	$3,16 \cdot 10^{-5}$	$3,16 \cdot 10^{-4}$	$3,16 \cdot 10^{-3}$
10^{-5}	10^{-4}	10^{-3}	10^{-2}
$3,16 \cdot 10^{-5}$	$3,16 \cdot 10^{-4}$	$3,16 \cdot 10^{-3}$	$3,16 \cdot 10^{-2}$

Tabelle 5.10: *HR* für latente Gefährdungen in Gefährdungen je Stunde

terschätzung eingehen. Es handelt sich um keine Grenzwertbetrachtung.

Im Rahmen der Unfallwahrscheinlichkeitsermittlung wird nicht betrachtet, dass der Fahrdienstleiter oder andere am Bahnbetrieb beteiligte Personen von außen auf den Zug bzw. den Betrieb Einfluss nehmen. Die Unsicherheit bei der Abschätzung dieser Wahrscheinlichkeiten ist groß und kann statistisch nicht belegt werden. Es wurde zur Beschreibung der Reduktionsmöglichkeiten im Falle des Zusammenstoßes ein betrieblicher Ansatz gewählt, der davon ausgeht, dass die Person vor Ort, d.h. der Triebfahrzeugführer, im Moment der Offenbarung einer Fehlfunktion unverzüglich und sofort im Rahmen der betrieblichen Möglichkeiten handelt. Es wird nicht davon ausgegangen, dass zur betrachteten Fehlfunktion noch ein Versagen des Triebfahrzeugführers bei der Unfallverhinderung hinzukommt. Die Abschätzung der Reduktionsmöglichkeiten für den Entgleisungsfall erfolgt basierend auf der Geschwindigkeitsdifferenz zwischen zulässiger und gefahrener Geschwindigkeit.

Für Gefährdungen, bei denen es ausgeschlossen ist, dass der Triebfahrzeugführer durch sein Handeln einen Einfluss auf die Unfallwahrscheinlichkeit hat, ist stets die höchste Unfallwahrscheinlichkeitsklasse zu wählen.

Für die Risikographerstellung wurden Informationen zu Unfällen in der Literatur ausgewertet. Im Unterschied zu einer Unfallstatistik stehen nur wenige Unfalldatensätze zur Verfügung. Nichtsdestotrotz konnte auf diese Weise das grundsätzliche Vorgehen gezeigt werden. Es ist davon auszugehen, dass es sich um eine Abschätzung zur sicheren Seite handelt, da in der Literatur der Schwerpunkt auf schweren Unfällen liegt und Ereignisse mit vergleichsweise geringen Auswirkungen vernachlässigt, d.h. nicht erwähnt werden. Wenn Unfallstatistiken zur Verfügung stehen, kann eine Auswahl der Unfälle z.B. entsprechend des betrieblichen Umfelds erfolgen.

5.14.3 Diskussion der Kalibrierung und Ergebnisermittlung

Die Kalibrierung erfolgte mit dem RAC-TS Kriterium. Deshalb gelten die mit dem Risikographen ermittelten Ergebnisse nur für technische Komponenten. Der Einfluss des Menschen wird nur dann betrachtet, wenn dies ein äußeres, von der betrachteten Komponente unabhängiges Ereignis ist. Dies ist bei der Systemdefinition entsprechend zu berücksichtigen.

Die angegebenen zulässigen Gefährdungsraten wurden nicht berechnet, sondern zugewiesen. Es ist daher nicht möglich, mit dem Risikographen bzw. den im Risikographen angegebe-

nen Parametern einen Risikowert zu berechnen und mit realen Risikowerten zu vergleichen.

Im Unterschied zu den bisher in der Literatur zu findenden Risikographen handelt es sich bei dem konstruierten Risikographen um einen symmetrischen Graphen. Dies bedeutet, dass stets alle Parameter zu beurteilen sind, um ein Ergebnis zu ermitteln. Es wird vermutet, dass die Asymmetrie bei bestehenden Risikographen auf die Berücksichtigung von Risikoaversion zurückgeht, die in die Konstruktion des Beispielrisikographen nicht eingeflossen ist.

5.14.4 Überlegungen zur Genauigkeit der Risikoabschätzung

In DIN EN 61508-1 (2002) erfolgt eine Zuordnung der Ausfallraten zu den Sicherheitsintegritätsleveln. Dabei werden feste, halboffene Intervalle definiert. Als Beispiel wird hier eine *Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung* betrachtet. Bei einer *Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde* von $\geq 10^{-8}$ bis $< 10^{-7}$ wird der Sicherheitsintegritätslevel 3 zugeordnet. Dies bedeutet, dass bei einem ermittelten Ausfall von 10^{-7} pro Stunde die Zuweisung zum SIL 2 erfolgt, bei 10^{-8} zu SIL 3 und bei $10^{-8} + x$ zu SIL 4 (x sei ein beliebiger, positiver Wert).

Es bietet sich an, diese Grenzwerte auch als Grenzen für die Risikographergebnisermittlung zu nutzen. Dabei kann die Frage aufkommen, ob eine scharfe Trennung der Ergebnisklassen zulässig ist oder ob dies aufgrund der Ungenauigkeiten in der Parameterabschätzung nicht sinnvoll ist.

Es ist ein Vorteil der quantitativen Risikoberechnung bzw. der quantitativen Parameterermittlung, dass basierend auf den zugrunde liegenden Daten eine statistische Betrachtung der Zuverlässigkeit der angenommenen Werte und darauffolgend des abgeschätzten Risikos erfolgen kann. Grundsätzlich wäre es möglich, anhand der ermittelten Werte bei einer Risikoberechnung eine „Grauzone“ rund um die Grenzwerte zu definieren, in denen die Zuweisung des SIL abhängig von den Ergebnissen der statistischen Betrachtung erfolgt. Allerdings ist ein solches Vorgehen aus der Literatur bisher nicht bekannt.

Eine quantitative Genauigkeitsbetrachtung ist bei qualitativen Methoden nicht möglich. Es wäre denkbar, dass mit einer Risikoabschätzungsmethode ermittelte Ergebnis durch einen Sicherheitsbeiwert, der eine Aussage über das Vertrauen, welches der Anwender in seine Schätzungen hat, abzusichern. Dieses Vorgehen wird im Rahmen der Arbeit nicht verfolgt. Um abzuschätzen, ob es zulässig ist, die Grenzwerte aus der Norm als Ergebnisklassengrenzwerte zu verwenden, muss betrachtet werden, welche Überlegungen der Wahl der Parameterklassen zu Grunde liegen. Wie bereits ausgeführt wurde, ist die Abschätzung des Parameters Schadensausmaß eine Abschätzung zur sicheren Seite. Es wird ein hohes, unter ungünstigen betrieblichen Bedingungen zu erwartendes Schadensausmaß abgeschätzt. Für die Unfallwahrscheinlichkeit wird von durchschnittlichen, typischen Reduktionsmöglichkeiten ausgegangen. Jedoch sind die Reduktionsmöglichkeiten, die überhaupt im Rahmen des Parameters betrachtet werden können, begrenzt. Eine Vielzahl von Einflüssen wird nicht erfasst, hat aber dennoch im Einzelfall große Bedeutung zur Unfallvermeidung. Daher kann davon ausgegangen werden, dass die tatsächliche Unfallwahrscheinlichkeit deutlich niedriger ist, als die im Rahmen des Risikographen angenommene Unfallwahrscheinlichkeit.

Die Zahlenwerte für den menschlichen Fehler wurden der Literatur entnommen. Es können keine Aussagen getroffen werden, ob diese Werte zur sicheren Seite ermittelt wurden, d.h. einen Zuschlag für Ungenauigkeiten bei der Anwendung beinhalten. Da sie jedoch für Screeningmethoden Anwendung finden, ist davon auszugehen, dass die Werte auf der sicheren Seite liegen.

Es wird geschlussfolgert, dass das mit einem semi-qualitativen Risikographen abgeschätzte Risiko eine Abschätzung zur sicheren Seite, d.h. größer als das tatsächlich vorhandene Risiko ist. Dies bedeutet, dass die ermittelte Gefährdungsrate ebenfalls zur sicheren Seite abgeschätzt ist, d.h. niedriger ist als bei einer detaillierteren Betrachtung notwendig. Daher erscheint es zulässig, wenn die Grenzwerte aus DIN EN 61508-1 (2002) als Grenzwerte übernommen werden. Es muss kein Zuschlag für die Ungenauigkeit der Ergebnisse berücksichtigt werden.

5.14.5 Folgeunfälle

Unfälle können Auslöser für Folgeunfälle sein. Es wird im Rahmen dieser Arbeit davon Abstand genommen, diesen kausalen Zusammenhang im Risikographen abzubilden. Aus jedem Unfall kann sich ein Folgeunfall entwickeln, der ähnlich wie der ursprüngliche Unfall analysiert werden kann. Prinzipiell kann so eine Argumentationskette immer fortgeschrieben werden, da beispielsweise an der Unfallstelle von zwei Unfällen theoretisch noch ein dritter Unfall, durch die ersten Unfälle ausgelöst, sich ereignen kann. Es kann angenommen werden, dass die Wahrscheinlichkeit für einen Folgeunfall geringer ist als die Wahrscheinlichkeit für den Ursprungsunfall. Aufgrund der Ungenauigkeiten in der Parameterschätzung ist die Zuverlässigkeit der Aussagen und Abschätzungen mit zunehmender Szenariolänge immer geringer. Deshalb erscheint es sinnvoll, nach dem ersten Unfall die Betrachtung abzubrechen.

5.15 Zusammenfassung

5.15.1 Annahmen bei der Konstruktion des Beispielrisikographen

In der vorliegenden Arbeit wurde ein generisch-anwendungsbezogener Risikograph erstellt, der als Ergebnis eine einzuhaltende Gefährdungsrate für eine, eine Funktion ausführende, Komponente liefert. In der folgenden Übersicht sind die wesentlichen, der Konstruktion zu Grunde liegenden, Annahmen zusammengestellt.

Der Konstruktion liegt ein qualitatives Risikomodell zu Grunde. Dieses wurde wie folgt definiert: Es wird unter den Randbedingungen aus dem Betrieb Nichtbundeseigener Eisenbahnen das kollektive Risiko der Reisenden in einem Zug aufgrund der Fehlfunktion sichernder technischer Funktionen ermittelt. Eine Funktion ist laut DIN EN 50129 (2003) eine Art von Aktion oder Tätigkeit, durch die ein Produkt seinen beabsichtigten Zweck erfüllt. Dem Risikographen liegt die folgende Formel mit R dem Risiko, HR der Gefährdungsrate, DE dem Parameter zum Abbilden von Aussetzungszeit und Gefährdungsdauer, C der Unfallwahrscheinlichkeit und F dem Schadensausmaß zu Grunde:

$$R = HR \cdot DE \cdot C \cdot F \tag{5.10}$$

Es wird ein komponentenbezogenes, kollektives Risiko ermittelt.
Für die Ableitung der Gefährdungen gilt:

- Eine Gefährdung ist eine Fehlfunktion zur unsicheren Seite mit einem Potential von analyserelevantem Schaden. Für den Beispielrisikographen ist Personenschaden der analyserelevante Schaden.

- Es wird zwischen latenten und direkten Gefährdungen unterschieden.

  - Es werden nur solche latenten Gefährdungen betrachtet, die durch das Zusammentreffen von genau zwei Ereignissen entstehen.
  - Es wird davon ausgegangen, dass es sich bei den Ereignissen um ein technisches Versagen und einen menschlichen Fehler handelt.

- Es wird nicht davon ausgegangen, dass gefährliche Zustände durch systeminterne Prozesse automatisch und ohne Aufdeckung in sichere Zustände zurückgeführt werden.

- Die Gefährdungsableitung erfolgt durch Negierung der Funktion oder durch detaillierte Ausfallbetrachtung.

Für die Konstruktion des Parameters Schaden wurden die folgenden Randbedingungen gesetzt:

- Es wird Personenschaden betrachtet. Es wird davon ausgegangen, dass eine Begrenzung des Personenschadens implizit auch eine Begrenzung anderer Schadensarten, im Besonderen von Sach- und Imageschaden, erfolgt.

- Es ist eine hohe, tatsächlich im normalen Betrieb zu erwartende Schadenshöhe abzuschätzen.

- Es wird eine implizite Schadensschätzung vorgenommen. Es wird ein unfallstatistikbasierter Ansatz verfolgt, der einen Zusammenhang zwischen Energieäquivalent, Schadensausmaß und Unfallszenario hergestellt.

- Es wird für die Parameterklassenermittlung eine Aussage zur Geschwindigkeit und zum Unfallszenario benötigt. Alle anderen Einflüsse werden durch den unfallstatistikbasierten Ansatz implizit berücksichtigt.

- Es wird davon ausgegangen, dass die in der Literatur aufgenommenen Unfälle im Allgemeinen besonders schwere Unfälle sind. Es wird der Definition, dass *ein typisches, hohes Schadensausmaß unter für das Schadensausmaß ungünstigen, jedoch betrieblich häufig und typischerweise vorkommenden Bedingungen* zu wählen ist, genüge getan. Der Unfall Eschede wurde von der Betrachtung ausgeschlossen.

- Der Gesamtschaden wird basierend auf der Zahl der schwer verletzten und getöteten Personen ermittelt in $\text{Opfer} = \text{Tote} + \frac{\text{Schwerverletzte}}{10}$.

- Bei einer pauschalen Angabe des Schadensausmaßes in der Literatur wird angenommen, dass ein Drittel der Personen schwer und zwei Drittel der Personen leicht verletzt wurden.

- Für die mathematische Approximation des Zusammenhangs von Energieäquivalent und Schadensausmaß wird davon ausgegangen, dass der erste Teil der Kurve durch eine lineare Funktion abgebildet werden kann und der zweite Teil der Kurve durch eine exponentielle Funktion.

Der Konstruktion des Parameters Unfallwahrscheinlichkeit erfolgte basierend auf den folgenden Annahmen:

- Es wird von einer unbedingten Offenbarung ausgegangen. Der Fall, dass eine Gefährdung auftritt, die ohne Offenbarung in einen sicheren Zustand überführt wird, wird nicht betrachtet.

- Es sind mittlere, durchschnittliche (typische) Reduktionsmöglichkeiten zu betrachten.
- Physikalische Maßnahmen werden nicht im Rahmen der Reduktionsfaktoren zum Ansatz gebracht.
- Es werden keine zufälligen, ggf. vorteilhaften Einflüsse aus z.B. der Umgebung berücksichtigt.
- Es wird nur das Handeln des Triebfahrzeugführers als Einfluss auf die Unfallwahrscheinlichkeit berücksichtigt.
- Maßgeblich für die Unfallwahrscheinlichkeit bei Entgleisungen ist Entgleisungsursache (Unstetigkeitsstellen im Fahrweg) bzw. die Differenz zwischen gefahrener und zulässiger Geschwindigkeit. Maßgeblich für die Unfallwahrscheinlichkeit bei Zusammenstößen ist die Wahrscheinlichkeit, dass zwei betroffene Fahrzeuge rechtzeitig zum Halten gebracht werden können.

Der Konstruktion des Parameters Aussetzungszeit/Gefährdungsdauer wurden die folgenden Randbedingungen zu Grunde gelegt:

- Es wird angenommen, dass die Zeit, die ein Zug einer Komponente ausgesetzt ist, auf der sicheren Seite abgeschätzt werden kann mit der Zeit, die der Zug den entsprechenden Fahrstraßenabschnitt belegt.
- Es wird abstrahiert, dass ein Zug betrachtet wird, der die zu analysierende Komponente so oft innerhalb einer Betriebsstunde befährt, wie die Gesamtheit aller Züge laut Betriebsprogramm dies tun würde. Es wird davon ausgegangen, dass der Zug zwischen zwei Stationen pendelt. Er fährt mit der laut Betriebsprogramm bzw. Streckeninformation vorgegebenen Geschwindigkeit.
- Bei Gefährdungsbestehenszeiten, die über 100 Stunden hinausgehen, ist das Ergebnis der Analyse mit dem Risikographen nur nach Rücksprache mit z.B. der Genehmigungsbehörde anwendbar.

Der Konstruktion des Parameters menschliche Fehlerwahrscheinlichkeit unter Berücksichtigung der folgenden Randbedingungen:

- Es werden die Zahlenwerte nach VDI 4006, Blatt 2 (2003) zu Grunde gelegt.
- Es werden drei Klassen für menschliche Fehlerwahrscheinlichkeit unterschieden.

Der Risikograph ist die Kombination der diskutierten Parameter entsprechend dem Risikomodell.

- Der Risikograph wurde mit dem Risikoakzeptanzkriterium für technische Systeme nach Verordnung EG Nr. 352/ (2009) kalibriert.
- Es wurde eine Parameterklassenkombination ermittelt, die dem durch RAC-TS beschriebenen Szenario entspricht (Benchmark-Szenario).
- Die Ergebnisableitung für weitere Parameterklassenkombinationen erfolgte ausgehend von der Benchmark-Parameterklassenkombination durch Anwendung des Faktors $\sqrt{10}$ bzw. 10 in einer Tabelle. Es wurde kein Risiko ermittelt.

5.15.2 Bedingungen für die Anwendung des Risikographen

Der Risikograph ist anzuwenden auf die aus unterschiedlichen Funktionen von Bahnsignalanlagen erwachsenden Gefährdungen. Vor Anwendung des Risikographen sind die folgenden Randbedingungen zu prüfen:

- Die zu analysierende Komponente und ihre Funktion muss dem Systemmodell nach Bild 5.2 entsprechen.
- Die Funktion muss der Definition für die Analyseebene entsprechen: Die Analyseebene ist definiert als Ebene, die alle diejenigen physischen Komponenten enthält, die entweder in Zusammenarbeit mit dem Stellwerk oder als selbständige Komponenten die Sicherheit eines Zuges durch ihr Wirken direkt herstellen.
- Es muss sich um eine technische Komponente handeln.

5.15.3 Vorgehen

Es kann zur Analyse mit dem Risikographen das Formular aus Bild 5.33 genutzt werden.

Es sind zunächst die relevanten Gefährdungen urch Negierung der Funktion oder durch detaillierte Ausfallbetrachtung abzuleiten. Eine Gefährdung ist eine Fehlfunktion zur unsicheren Seite mit einem Potential von analyserelevantem Schaden. Für den Beispielrisikographen ist Personenschaden der analyserelevante Schaden. Es ist zwischen latenten und direkten Gefährdungen zu unterscheiden.

Im Allgemeinen können für jede Gefährdung mehrere Unfallszenarien unterschieden werden.

- Im Risikographen können die folgenden Unfallszenarien analysiert werden: Zusammenstoß mit einem stehenden Zug bzw. Hindernis[7], Zusammenstoß mit einem Zug, welcher mit der Geschwindigkeit 50 km/h fährt (Bahnhof), Zusammenstoß mit einem Zug, welcher mit der Geschwindigkeit 80 km/h fährt (Strecke R 80) und Zusammenstoß mit einem Zug, welcher mit der Geschwindigkeit 120 km/h fährt (Strecke R 120)
- Flankenfahrten werden als Zusammenstöße betrachtet.

Zur Ermittlung der Parameterklasse Schaden (Bilder 5.34 und 5.35) werden Aussagen zur Geschwindigkeit des betrachteten Zugs und zum Unfallszenario benötigt. Bei der Ermittlung der Unfallwahrscheinlichkeitsklasse ist nach den Szenarien zu unterscheiden:

- Entgleisung: Es werden Aussagen zum Grund für die Entgleisung (stetiger/unstetiger Fahrweg) und zur gefahrenen und zulässigen Geschwindigkeit benötigt (Bild 5.36).
- Zusammenstoß: Es werden Aussagen zur Art der Schutzverletzung (Folgefahrschutz, Gegenfahrschutz; bei fehlendem Flankenschutz bzw. fehlendem Schutz vor einem Hindernis im Gleis sind zu behandeln als fehlender Gegenfahrschutz, wenn Zug 1 steht) und zur gefahrenen Geschwindigkeit benötigt (Bilde 5.37 und 5.38).

Zur Ermittlung des Parameters Aussetzungszeit/Gefährdungsdauer (Bild 5.40) sind beide Summanden getrennt zu betrachten.

[7] Im Folgenden wird davon ausgegangen, dass der Fall Zusammenstoß mit stehendem Zug alle anderen Zusammenstöße mit stehenden Objekten (Hindernissen) umfasst.

HR	MF_3 0,1	MF_2 0,01	MF_1 0,001
10^{-9}	10^{-8}	10^{-7}	10^{-6}
$3,16 \cdot 10^{-9}$	$3,16 \cdot 10^{-8}$	$3,16 \cdot 10^{-7}$	$3,16 \cdot 10^{-6}$
10^{-8}	10^{-7}	10^{-6}	10^{-5}
$3,16 \cdot 10^{-8}$	$3,16 \cdot 10^{-7}$	$3,16 \cdot 10^{-6}$	$3,16 \cdot 10^{-5}$
10^{-7}	10^{-6}	10^{-5}	10^{-4}
$3,16 \cdot 10^{-7}$	$3,16 \cdot 10^{-6}$	$3,16 \cdot 10^{-5}$	$3,16 \cdot 10^{-4}$
10^{-6}	10^{-5}	10^{-4}	10^{-3}
$3,16 \cdot 10^{-6}$	$3,16 \cdot 10^{-5}$	$3,16 \cdot 10^{-4}$	$3,16 \cdot 10^{-3}$
10^{-5}	10^{-4}	10^{-3}	10^{-2}
$3,16 \cdot 10^{-5}$	$3,16 \cdot 10^{-4}$	$3,16 \cdot 10^{-3}$	$3,16 \cdot 10^{-2}$

Tabelle 5.11: Ergebnisermittlung bei Berücksichtigung der menschlichen Fehlerwahrscheinlichkeit

- Parameter E: Es werden Aussagen zur Anzahl der Züge je Stunde, zur gefahrenen Geschwindigkeit und zur anzunehmenden Blocklänge benötigt (Bild 5.39). Wird ein Szenario im Bahnhof als relevant betrachtet, so ist der in Tabelle 5.25 angegebene Zahlenwert zu verdoppeln. Wird der so ermittelte Wert größer eins, ist eins anzunehmen.
- Parameter D: Die Gefährdungsdauer ist abzuschätzen.

Es ist zunächst mittels Risikograph eine zulässige Gefährdungsrate für die betrachtete Funktion der Komponente unter Annahme des Unfallszenarios abzuleiten (Bild 5.41). Für latente Gefährdungen kann in einem zweiten Schritt die menschliche Fehlerwahrscheinlichkeit berücksichtigt (Tabelle 5.11) und so die von der Technik einzuhaltende Gefährdungsrate reduziert werden.

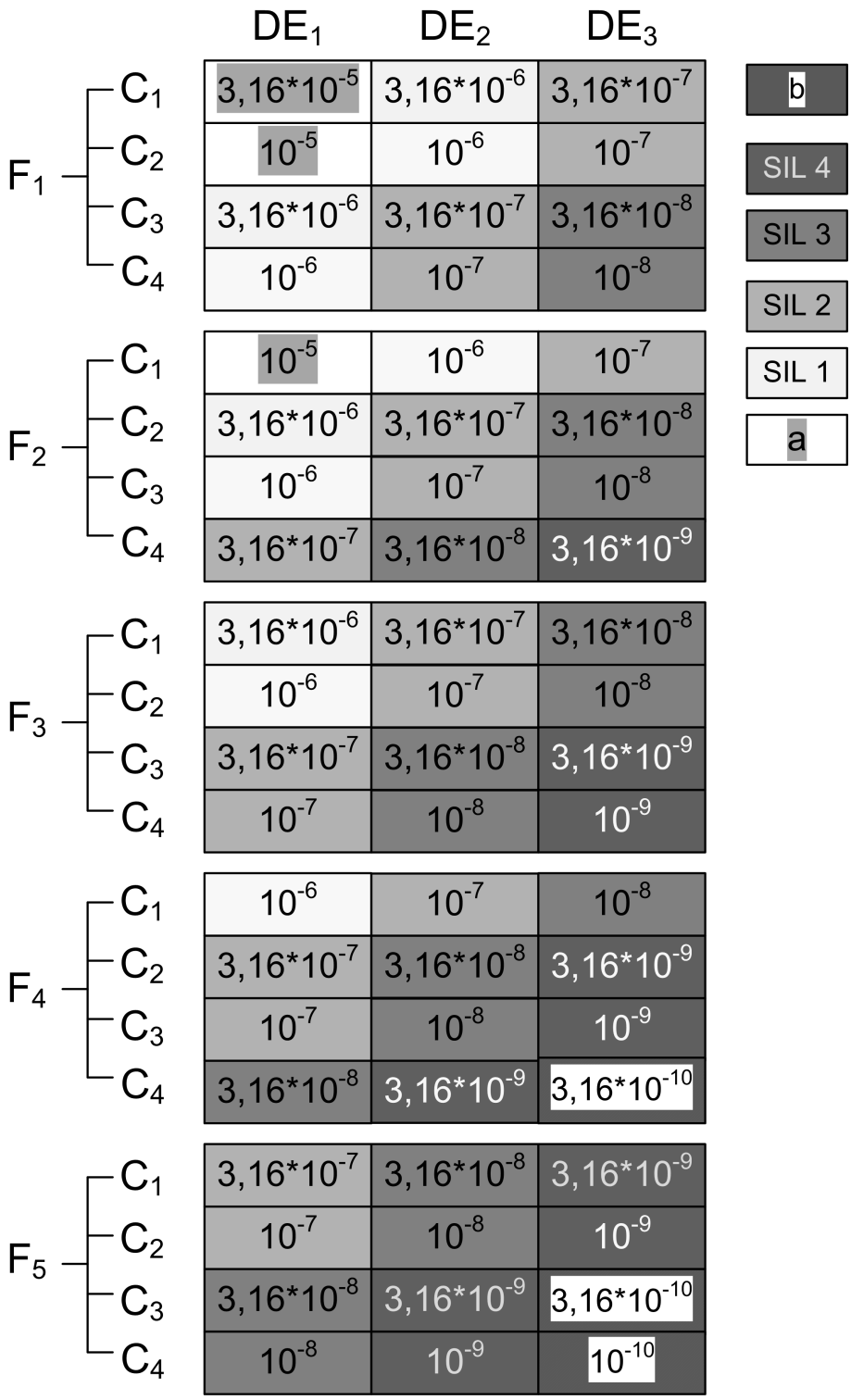

Bild 5.32: Der Beispielrisikograph (Zahlenwerte in Gefährdungen je Stunde)

Benennung der Gefährdung:						
Eingangsgrößen						
Streckengeschwindigkeit [km/h]						
Abzweiggeschwindigkeit [km/h]						
Anzahl Züge je Stunde und Abschnitt						
Blocklänge [km]						
Infrastruktur						
Wahl des Schadensparameters (lt. Diagramm)		**F_1**	**F_2**	**F_3**	**F_4**	**F_5**
ZS mit einem stehenden Zug						
ZS mit einem Zug, welcher mit der Geschwindigkeit 50 km/h fährt (Bahnhof)						
ZS mit einem Zug, welcher mit der Geschwindigkeit 80 km/h fährt (Strecke R 80)						
ZS mit einem Zug, welcher mit der Geschwindigkeit 120 km/h fährt (Strecke R 120)						
Entgleisung 75 %						
Entgleisung 25 %						
Wahl des Parameters Unfallwahrscheinlichkeit (lt. Diagramm)		**C_1**	**C_2**	**C_3**	**C_4**	
für Entgleisungen bei überhöhter Geschwindigkeit (Eingangsgröße: $v_{strecke}/v_{abzweig}$)						
für Entgleisungen, wenn Fahrweg nicht zur Verfügung steht (unstetiger Fahrweg)						
Verletzung des Folgefahrschutzes						
ZS mit einem stehenden Zug						
ZS mit einem Zug, welcher mit der Geschwindigkeit 50 km/h fährt (Bahnhof)						
ZS mit einem Zug, welcher mit der Geschwindigkeit 80 km/h fährt (Strecke R 80)						
ZS mit einem Zug, welcher mit der Geschwindigkeit 120 km/h fährt (Strecke R 120)						
Verletzung des Gegenfahrschutzes/ Flankenschutzes						
ZS mit einem stehenden Zug						
ZS mit einem Zug, welcher mit der Geschwindigkeit 50 km/h fährt (Bahnhof)						
ZS mit einem Zug, welcher mit der Geschwindigkeit 80 km/h fährt (Strecke R 80)						
ZS mit einem Zug, welcher mit der Geschwindigkeit 120 km/h fährt (Strecke R 120)						
Wahl des Parameters Gefährdungsdauer/Aussetzungszeit		**DE_1**	**DE_2**	**DE_3**		
Gefährdungsdauer (in [h], Schätzwert)						
Aussetzungszeit (in [h], aus Tabelle)						
Parameter lt. Diagramm						
Wahl des Parameters menschlicher Fehler		**MF_1**	**MF_2**	**MF_3**		
Einfache und häufig durchgeführte Aufgaben bei minimalem Stress (MF_1) Komplexere Aufgaben unter Zeitdruck, wobei eine gewisse Sorgfalt bei der Durchführung notwendig ist (MF_2) Komplexere, ungewohnte Aufgaben mit geringer Rückmeldung über den Erfolg und die Gefahr, Zerstörungen zu verursachen (MF_3)						

Bild 5.33: Formular zur Ermittlung der Parameterklassen im Rahmen der Risikographanalyse

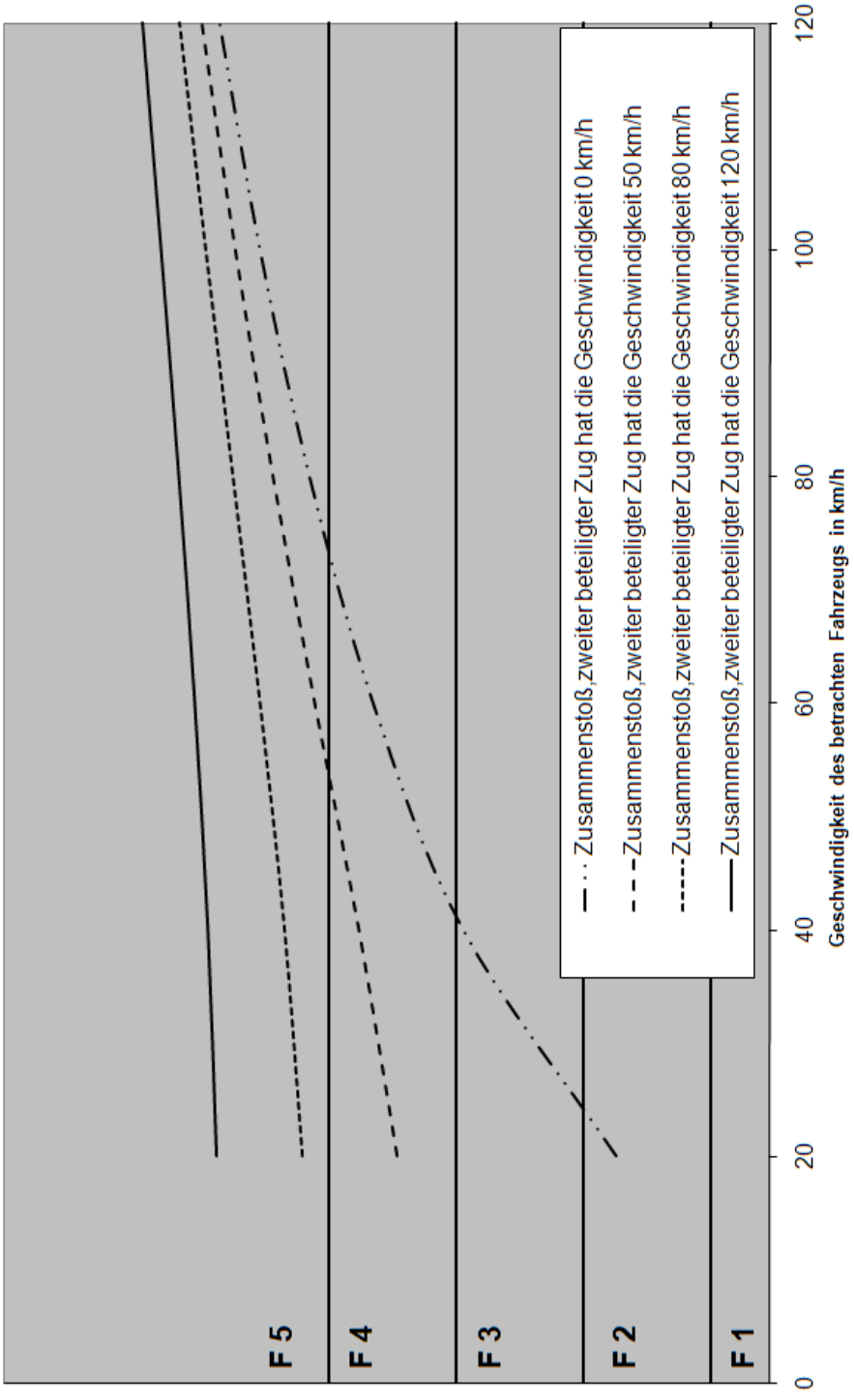

Bild 5.34: Diagramm zur Ermittlung der Schadensklassengrenzen bei Zusammenstößen

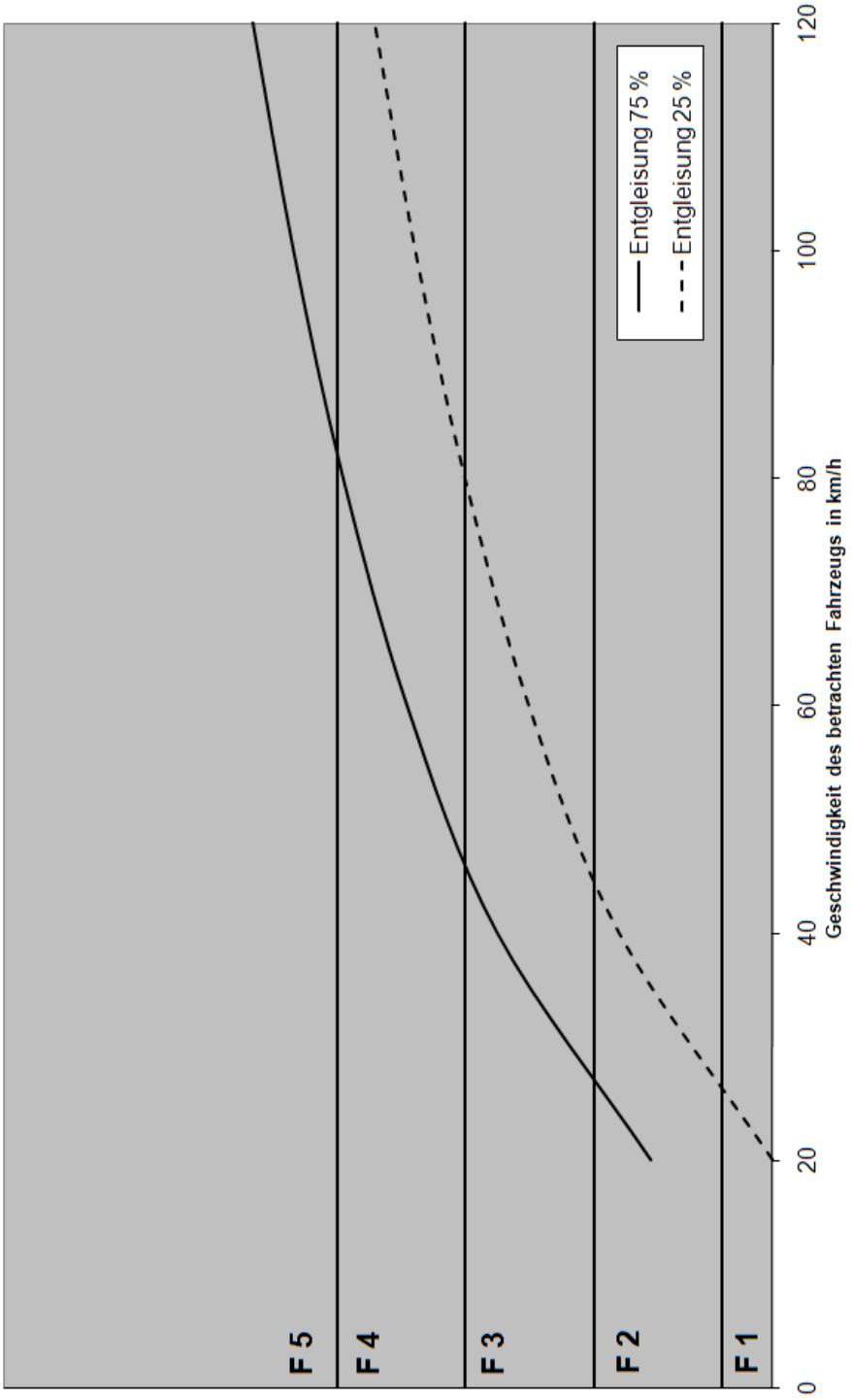

Bild 5.35: Diagramm zur Ermittlung der Schadensklassengrenzen bei Entgleisungen

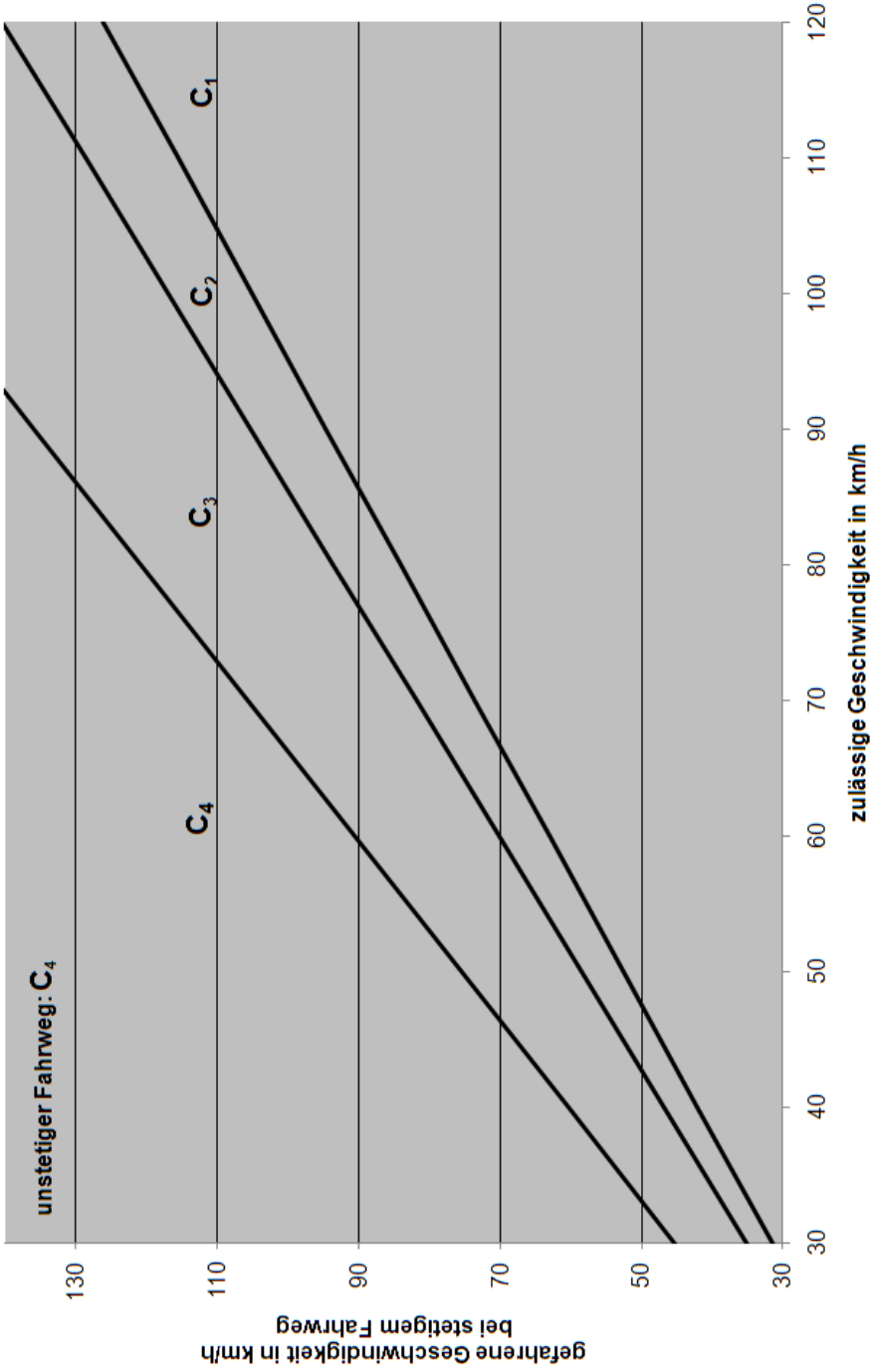

Bild 5.36: Diagramm zur Ermittlung der Unfallwahrscheinlichkeit für potentielle Entgleisungen

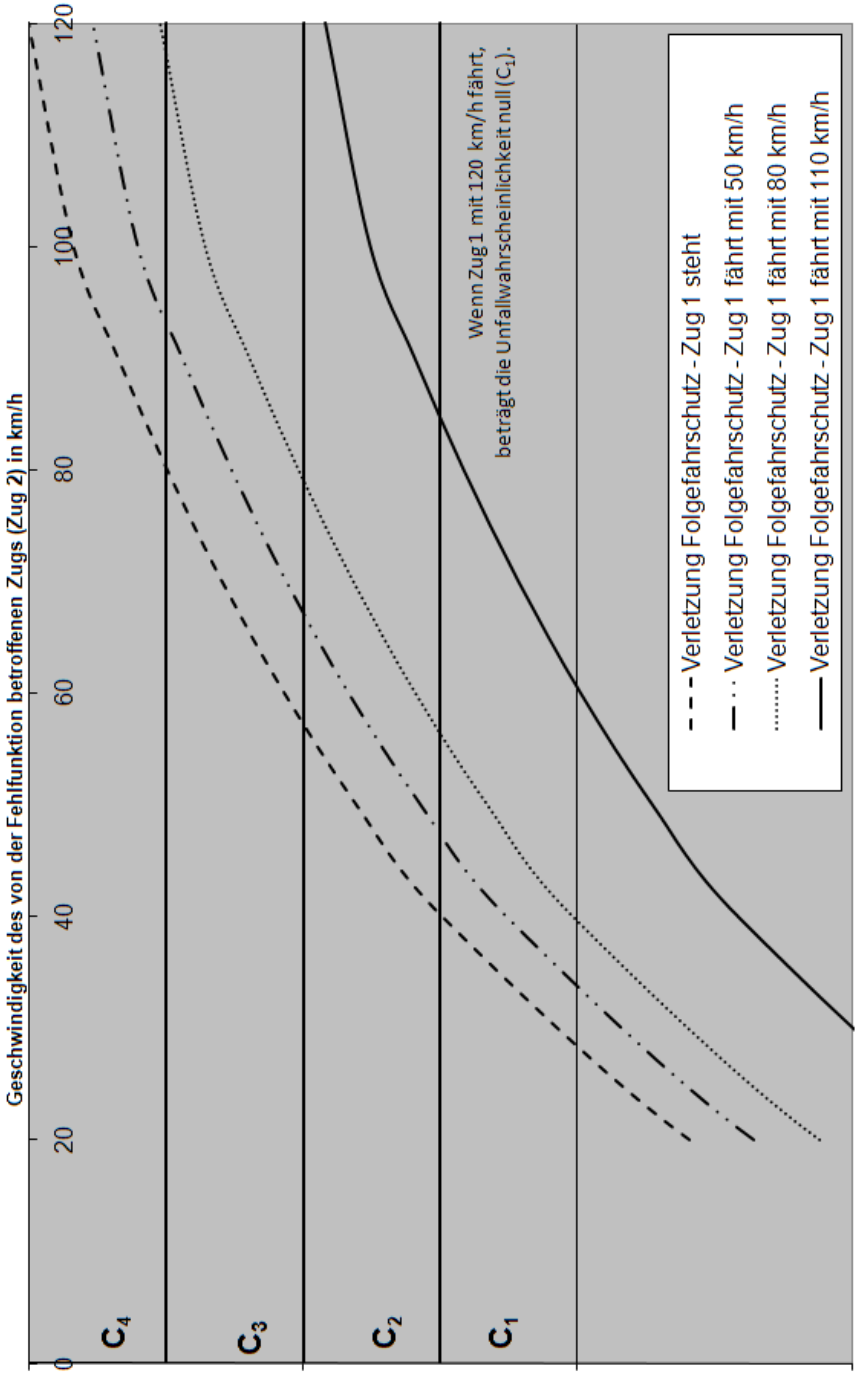

Bild 5.37: Diagramm zur Ermittlung der Unfallwahrscheinlichkeit bei Verletzungen des Folgefahrschutzes

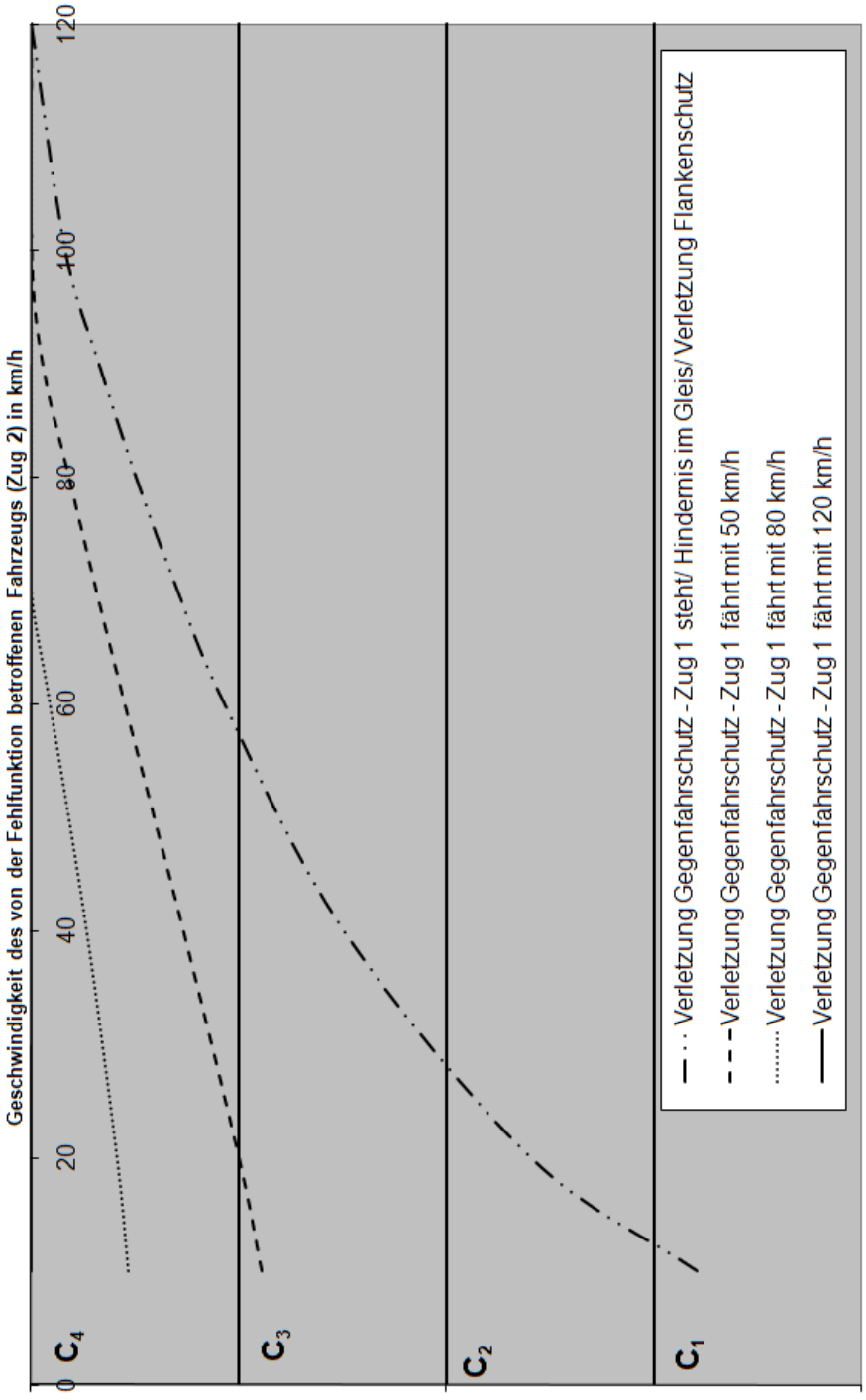

Bild 5.38: Diagramm zur Ermittlung der Unfallwahrscheinlichkeit bei Verletzungen des Gegenfahrschutzes

	Anzahl Züge pro Stunde					
	1	2	3	4	5	6
Wert für E bei v = 50 km/h						
Blocklänge 2000 m	0,075	0,150	0,226	0,301	0,376	0,451
Blocklänge 5000 m	0,135	0,270	0,406	0,541	0,676	0,811
Blocklänge 10000 m	0,235	0,470	0,706	0,941	1,000	1,000
Wert für E bei v = 80 km/h						
Blocklänge 2000 m	0,048	0,096	0,144	0,191	0,239	0,287
Blocklänge 5000 m	0,085	0,171	0,256	0,341	0,427	0,512
Blocklänge 10000 m	0,148	0,296	0,444	0,591	0,739	0,887
Wert für E bei v = 100 km/h						
Blocklänge 2000 m	0,039	0,077	0,116	0,155	0,194	0,232
Blocklänge 5000 m	0,069	0,137	0,206	0,275	0,344	0,412
Blocklänge 10000 m	0,119	0,237	0,356	0,475	0,594	0,712
Wert für E bei v = 120 km/h						
Blocklänge 2000 m	0,033	0,065	0,098	0,131	0,163	0,196
Blocklänge 5000 m	0,058	0,115	0,173	0,231	0,288	0,346
Blocklänge 10000 m	0,099	0,199	0,298	0,397	0,497	0,596

Bild 5.39: Berechnung des Parameters E

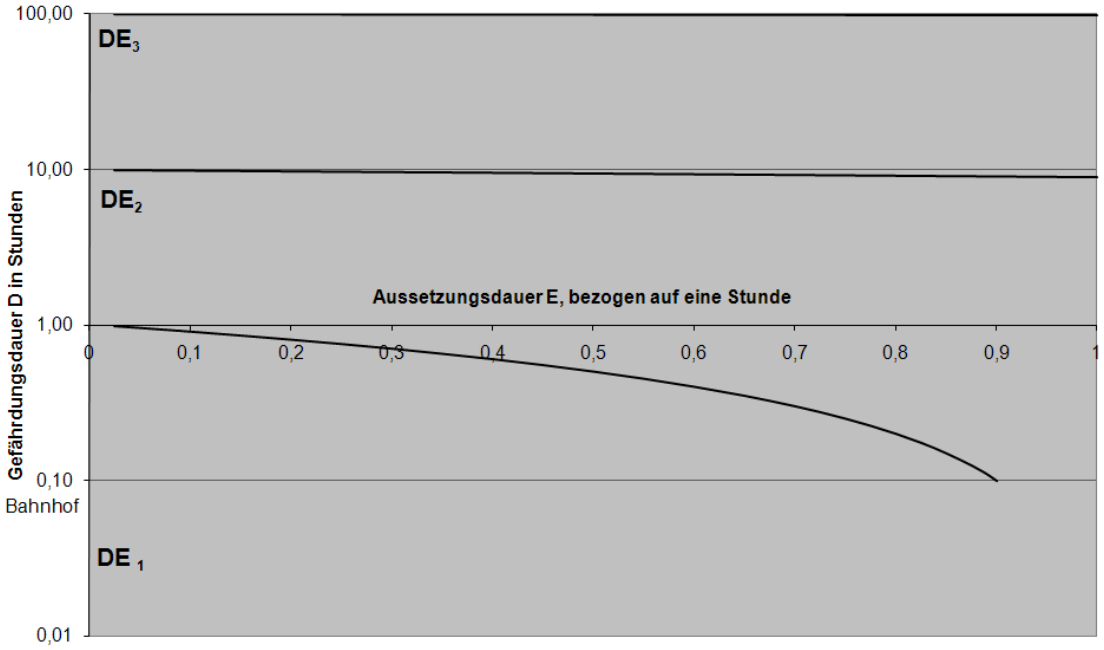

Bild 5.40: Diagramm zur Ermittlung des Parameters DE

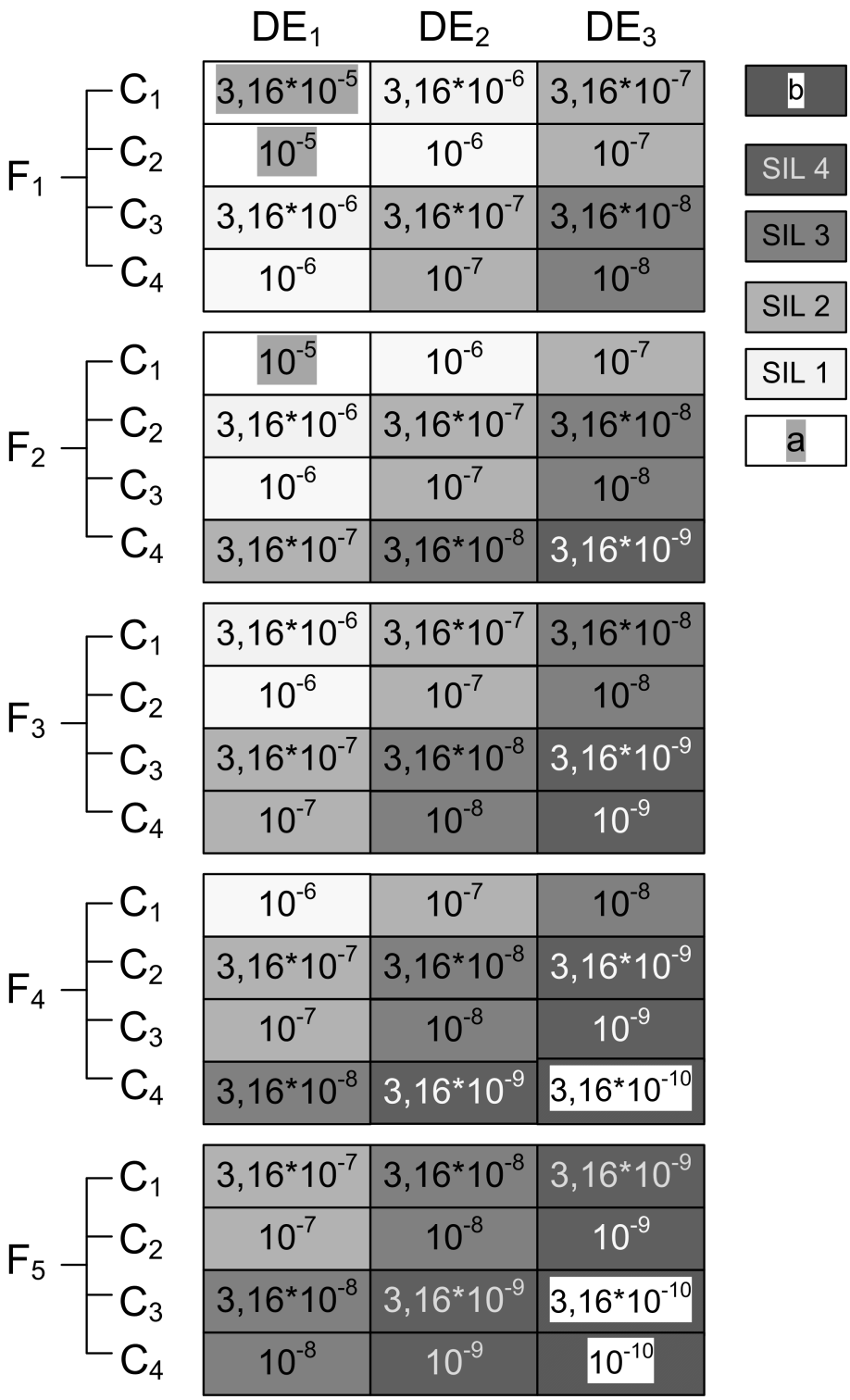

Bild 5.41: Der Beispielrisikograph

Kapitel 6

Anwendung des Risikographen

6.1 Prüfung der Anwendbarkeit

Um die Anwendung des Risikographen zu demonstrieren, werden zwei Komponenten analysiert: Hauptsignal und Fahrzeuggerät der punktförmigen Zugbeeinflussung, im Folgenden nur als punktförmige Zugbeeinflussung bezeichnet. Die Komponenten wurden ausgewählt, da ihre Funktionalität einfach zu beschreiben ist und die Auswirkungen verschiedener Einflüsse (unterschiedliche Geschwindigkeiten, latente und direkte Gefährdung) auf die Analyse präsentiert werden können.

Die Funktionen der Komponenten werden wie folgt (zum Teil basierend auf Pachl (2009)) abgeleitet:

- Hauptsignal: Signal, durch das im Regelbetrieb die Einfahrt eines Zuges in den auf das Signal folgenden Gleisabschnitt zugelassen wird, wenn alle Bedingungen für das Befahren des Gleisabschnitts erfüllt sind.

- punktförmige Zugbeeinflussung: Sicherungsanlage, um beim Abweichen von der erlaubten Fahrweise Schutzreaktionen (Zwangsbremsungen) auszulösen.

Es ist zu prüfen, ob die Komponente und ihre Funktion dem Systemmodell entsprechen, ob die Analyseebene eingehalten wird und ob es sich um eine technische Komponente handelt.

- Das Komponenten haben eine sichernde Funktion. Ihre Beachtung bzw. Nichtbeachtung hat direkt Auswirkungen auf den Betriebsablauf des Zugs. Es werden Züge mit Reisenden auf der Infrastruktur Nichtbundeseigener Eisenbahnen betrachtet. Es wird eine Maximalgeschwindigkeit von 120 km/h angenommen. Die Komponenten mit ihren Funktionen entsprechen dem Systemmodell.

- Die Analyseebene ist definiert als Ebene, die alle diejenigen physischen Komponenten enthält, die entweder in Zusammenarbeit mit dem Stellwerk oder als selbständige Komponenten die Sicherheit eines Zugs durch ihr Wirken direkt herstellen. Die Komponenten mit ihren Funktionen entsprechen der Analyseebene.

- Es muss sich um eine technische Komponente handeln. Es handelt sich bei den ausgewählten Komponenten um technische Komponenten.

Die Komponenten können mit dem Risikographen analysiert werden.

6.2 Analyseebene - Gefährdungsermittlung

Aus den Funktionen können die Gefährdungen abgeleitet werden. Dies kann durch Negierung oder detaillierte Betrachtung der Gefährdungen erfolgen. Es wird der Weg der Gefährdungsableitung durch Negierung der Funktionen verfolgt:

- Hauptsignal: Es wird die Einfahrt eines Zuges in den auf das Signal folgenden Gleisabschnitt zugelassen, obwohl nicht alle Bedingungen für das Befahren des Gleisabschnitts erfüllt sind.

- punktförmige Zugbeeinflussung: Trotz Abweichung von der erlaubten Fahrweise wird keine Schutzreaktion ausgelöst.

Es ist zu prüfen, ob es sich bei den Gefährdungen um latente oder direkte Gefährdungen handelt.

Die Fehlfunktion des Hauptsignals ist eine direkte Gefährdung, da diese ohne weitere Fehlfunktionen oder menschliche Fehler zu einem Unfall führen kann.

Bei der Fehlfunktion der punktförmigen Zugbeeinflussung handelt es sich um eine latente Gefährdung, da es nur durch das Hinzukommen eines menschlichen Fehlers (z.B. Triebfahrzeugführer missachtet Signalbegriff) zu einem Unfall kommen kann.

6.3 Parameterabschätzung

Allgemeine Erläuterungen

Die Betriebsbedingungen werden anhand der DB-Streckenstandards (Richtlinie 413 (2002)) beschrieben. Es wird in Anlehnung an den Streckenstandard R 120 die Streckengeschwindigkeit 100 km/h gewählt. Als Abzweiggeschwindigkeit kann ein Werte zwischen 40 km/h und 60 km/h angenommen werden. Es wird der Wert 60 km/h gewählt. Es wird von einer zweigleisigen Strecke, Blocklänge 5 km und 2 Zügen je Stunde und Richtung ausgegangen.

6.3.1 Erläuterungen zur Gefährdung Hauptsignal

Zur Ermittlung der Parameterklassen wird das bereitgestellte Formular genutzt. Es werden keine Unfallszenarien ausgeschlossen. Es handelt sich um eine direkte Gefährdung, d.h. es müssen keine Angaben zur Wirkung menschlicher Fehler gemacht werden. Eine Übersicht der gewählten Parameterklassen gibt Bild 6.1 wieder. Um einen Vergleich mit den in VDV 332 (2008) ermittelten Ergebnissen zu ermöglichen, wird zusätzlich zum oben beschriebenen Szenario noch ein Szenario mit Geschwindigkeiten kleiner oder gleich 30 km/h betrachtet (Bild 6.2). Die Ableitung der Parameterklassen kann den Bildern 6.3 bis 6.9 entnommen werden. Es wird für die Ermittlung des Parameters E der Bahnhof als maßgebliche Infrastruktur angenommen. Dies bedeutet, dass laut Abschnitt 5.11 der Zahlenwert für E zu verdoppeln ist.

Es wird zunächst die Beurteilung für das Hauptsignal bei Streckengeschwindigkeit (Geschwindigkeit größer als 30 km/h) diskutiert. Es ist offensichtlich, dass es für den Parameter Schaden eine Häufung für die Parameterklasse F_5 gibt. Das einzige Unfallszenario, welches zu einer niedrigeren Bewertung führt, wird als nicht maßgeblich eingeschätzt, da Szenarien, die zu einer entsprechenden Entgleisung führen, eher selten zu erwarten sind. Für den Parameter Unfallwahrscheinlichkeit wird die häufigste Bewertung als maßgeblich angenommen. Es wird

der Parameter C_4 abgeschätzt. Dies ist eine Abschätzung zur sicheren Seite. Als Eingangsgröße für den Risikographen wird die Parameterkombination F_5, C_4 und DE_1 gewählt. Als Ergebnis wird eine tolerierbare Gefährdungsrate von 10^{-8} Gefährdungen je Betriebsstunde und Komponente (Bild 6.10) ermittelt. Dies entspricht SIL 3.

Die Beurteilung für die Gefährdung Hauptsignal bei Geschwindigkeiten kleiner oder gleich 30 km/h kann nicht so eindeutig erfolgen. Die Ergebnisse lassen nicht den Schluss zu, dass die Beurteilung einer Parameterkombination für die Ergebnisermittlung ausreichend ist. Es werden drei Szenarien gewählt, die als besonders wahrscheinlich angesehen werden.

- Szenario 1: Der betrachtete Zug fährt mit einer Geschwindigkeit kleiner oder gleich 30 km/h auf ein mit einem Zug besetztes Gleis ein: Es wird die Parameterkombination F_3, C_1 und DE_1 gewählt. Das Ergebnis ist eine tolerierbare Gefährdungsrate von $3,16 \cdot 10^{-6}$ Gefährdungen je Betriebsstunde und Komponente. Dies entspricht SIL 1.

- Szenario 2: Der betrachtete Zug fährt mit einer Geschwindigkeit kleiner oder gleich 30 km/h in den Bahnhof ein; ein zweiter Zug kommt ihm mit 50 km/h entgegen. Es wird die Parameterkombination F_4, C_3 und DE_1 gewählt. Das Ergebnis ist eine tolerierbare Gefährdungsrate von 10^{-7} Gefährdungen je Betriebsstunde und Komponente. Dies entspricht SIL 2.

- Szenario 3: Der betrachtete Zug fährt mit einer Geschwindigkeit kleiner oder gleich 30 km/h und entgleist in einer Weiche[1]. Es wird die Parameterkombination F_3, C_4 und DE_1 gewählt. Das Ergebnis ist eine tolerierbare Gefährdungsrate von 10^{-7} Gefährdungen je Betriebsstunde und Komponente. Dies entspricht SIL 2.

Die weitere Verarbeitung der Ergebnisse, z.B. die Ableitung eines Gesamtvorgabewertes ist abhängig von äußeren Randbedingungen und erfolgt nicht im Rahmen der Arbeit. Es ist möglich, als Vorgabewert für die Komponente beispielsweise den Maximalwert aus den ermittelten Werte zu wählen oder die Szenarien nach ihrer Häufigkeit zu wichten und einen gewichteten Gesamtwert zu abzuleiten.

6.3.2 Erläuterungen zur Gefährdung der punktförmigen Zugbeeinflussung

Für die von der Komponente Fahrzeuggerät der punktförmigen Zugbeeinflussung ausgehende Gefährdung werden die folgenden Unfallszenarien abgeleitet: Es kommt zu einer Entgleisung (wenn der Fahrweg nicht zur Verfügung steht) oder zu einem Zusammenstoß (wenn der fragliche Gleisabschnitt noch belegt ist).

Es handelt sich um eine latente Gefährdung, d.h. es kann nur zu einem Unfall kommen, wenn zur technischen Fehlfunktion ein menschlicher Fehler hinzu kommt.

Die betriebliche Situation bei einem Zusammentreffen von einer Fehlfunktion der punktförmigen Zugbeeinflussung und einem Fehler des Triebfahrzeugführers ist vergleichbar mit der Situation beim Überfahren eines fälschlicherweise Fahrt zeigenden Hauptsignals. In beiden Fällen befährt der Zug unzulässiger Weise einen Fahrwegabschnitt. Es wird zur Ableitung der zulässigen Gefährdungsrate für die Technik die für die Gefährdung Hauptsignal (Geschwindigkeit größer als 30 km/h) ermittelte Parameterkombination F_5, C_4 und DE_1 übernommen. Mit dem Risikographen wird das Ergebnis 10^{-8} Gefährdungen je Betriebsstunde ermittelt. Diese Gefährdungsrate kann durch Anwendung des Parameters menschliche Zuverlässigkeit

[1] Dies kann geschehen, wenn eine falsch liegenden Weiche spitz befahren wird.

Benennung der Gefährdung:						
Es wird die Einfahrt eines Zuges in den auf das Signal folgenden Gleisabschnitt zugelassen, obwohl nicht alle Bedingungen für das Befahren des Gleisabschnitts erfüllt sind.						
Eingangsgrößen						
Streckengeschwindigkeit [km/h]	100					
Abzweiggeschwindigkeit [km/h]	60					
Anzahl Züge je Stunde und Abschnitt	2					
Blocklänge [km]	5					
Infrastruktur	Bahnhof					
Wahl des Schadensparameters (lt. Diagramm)		**F_1**	**F_2**	**F_3**	**F_4**	**F_5**
ZS mit einem stehenden Zug						x
ZS mit einem Zug, welcher mit der Geschwindigkeit 50 km/h fährt (Bahnhof)						x
ZS mit einem Zug, welcher mit der Geschwindigkeit 80 km/h fährt (Strecke R 80)						x
ZS mit einem Zug, welcher mit der Geschwindigkeit 120 km/h fährt (Strecke R 120)						x
Entgleisung 75 %						x
Entgleisung 25 %					x	
Wahl des Parameters Unfallwahrscheinlichkeit (lt. Diagramm)		**C_1**	**C_2**	**C_3**	**C_4**	
für Entgleisungen bei überhöhter Geschwindigkeit (Eingangsgröße: $v_{strecke}/v_{abzweig}$)					x	
für Entgleisungen, wenn Fahrweg nicht zur Verfügung steht (unstetiger Fahrweg)					x	
Verletzung des Folgefahrschutzes						
ZS mit einem stehenden Zug			x			
ZS mit einem Zug, welcher mit der Geschwindigkeit 50 km/h fährt (Bahnhof)				x		
ZS mit einem Zug, welcher mit der Geschwindigkeit 80 km/h fährt (Strecke R 80)					x	
ZS mit einem Zug, welcher mit der Geschwindigkeit 120 km/h fährt (Strecke R 120)					x	
Verletzung des Gegenfahrschutzes/ Flankenschutzes						
ZS mit einem stehenden Zug					x	
ZS mit einem Zug, welcher mit der Geschwindigkeit 50 km/h fährt (Bahnhof)					x	
ZS mit einem Zug, welcher mit der Geschwindigkeit 80 km/h fährt (Strecke R 80)					x	
ZS mit einem Zug, welcher mit der Geschwindigkeit 120 km/h fährt (Strecke R 120)					x	
Wahl des Parameters Gefährdungsdauer/Aussetzungszeit		**DE_1**	**DE_2**	**DE_3**		
Gefährdungsdauer (in [h], Schätzwert)	0,1					
Aussetzungszeit (in [h], aus Tabelle)	0,27					
Parameter lt. Diagramm		x				
Wahl des Parameters menschlicher Fehler		**MF_1**	**MF_2**	**MF_3**		
Einfache und häufig durchgeführte Aufgaben bei minimalem Stress (MF_1) Komplexere Aufgaben unter Zeitdruck, wobei eine gewisse Sorgfalt bei der Durchführung notwendig ist (MF_2) Komplexere, ungewohnte Aufgaben mit geringer Rückmeldung über den Erfolg und die Gefahr, Zerstörungen zu verursachen (MF_3)		keine Angabe nötig				

Bild 6.1: Zusammenstellung der ermittelten Ergebnisse für die Gefährdung Hauptsignal

Benennung der Gefährdung:						
Es wird die Einfahrt eines Zuges in den auf das Signal folgenden Gleisabschnitt zugelassen, obwohl nicht alle Bedingungen für das Befahren des Gleisabschnitts erfüllt sind (Einfahrt mit 30 km/h).						
Eingangsgrößen						
Streckengeschwindigkeit [km/h]	100					
Abzweiggeschwindigkeit [km/h]	60					
Anzahl Züge je Stunde und Abschnitt	2					
Blocklänge [km]	5					
Infrastruktur	Bahnhof					
Wahl des Schadensparameters (lt. Diagramm)		**F_1**	**F_2**	**F_3**	**F_4**	**F_5**
ZS mit einem stehenden Zug				x		
ZS mit einem Zug, welcher mit der Geschwindigkeit 50 km/h fährt (Bahnhof)					x	
ZS mit einem Zug, welcher mit der Geschwindigkeit 80 km/h fährt (Strecke R 80)						x
ZS mit einem Zug, welcher mit der Geschwindigkeit 120 km/h fährt (Strecke R 120)						x
Entgleisung 75 %			x			
Entgleisung 25 %				x		
Wahl des Parameters Unfallwahrscheinlichkeit (lt. Diagramm)		**C_1**	**C_2**	**C_3**	**C_4**	
für Entgleisungen bei überhöhter Geschwindigkeit (Eingangsgröße: $v_{strecke}/v_{abzweig}$)				x	x	
für Entgleisungen, wenn Fahrweg nicht zur Verfügung steht (unstetiger Fahrweg)					x	
Verletzung des Folgefahrschutzes						
ZS mit einem stehenden Zug		x				
ZS mit einem Zug, welcher mit der Geschwindigkeit 50 km/h fährt (Bahnhof)		x				
ZS mit einem Zug, welcher mit der Geschwindigkeit 80 km/h fährt (Strecke R 80)		x				
ZS mit einem Zug, welcher mit der Geschwindigkeit 120 km/h fährt (Strecke R 120)		x				
Verletzung des Gegenfahrschutzes/ Flankenschutzes						
ZS mit einem stehenden Zug		x				
ZS mit einem Zug, welcher mit der Geschwindigkeit 50 km/h fährt (Bahnhof)				x		
ZS mit einem Zug, welcher mit der Geschwindigkeit 80 km/h fährt (Strecke R 80)					x	
ZS mit einem Zug, welcher mit der Geschwindigkeit 120 km/h fährt (Strecke R 120)					x	
Wahl des Parameters Gefährdungsdauer/Aussetzungszeit		**DE_1**	**DE_2**	**DE_3**		
Gefährdungsdauer (in [h], Schätzwert)	0,1					
Aussetzungszeit (in [h], aus Tabelle)	0,27					
Parameter lt. Diagramm		x				
Wahl des Parameters menschlicher Fehler		**MF_1**	**MF_2**	**MF_3**		
Einfache und häufig durchgeführte Aufgaben bei minimalem Stress (MF_1) Komplexere Aufgaben unter Zeitdruck, wobei eine gewisse Sorgfalt bei der Durchführung notwendig ist (MF_2) Komplexere, ungewohnte Aufgaben mit geringer Rückmeldung über den Erfolg und die Gefahr, Zerstörungen zu verursachen (MF_3)		keine Angabe nötig				

Bild 6.2: Zusammenstellung der ermittelten Ergebnisse für die Gefährdung Hauptsignal bei Geschwindigkeiten kleiner oder gleich 30 km/h

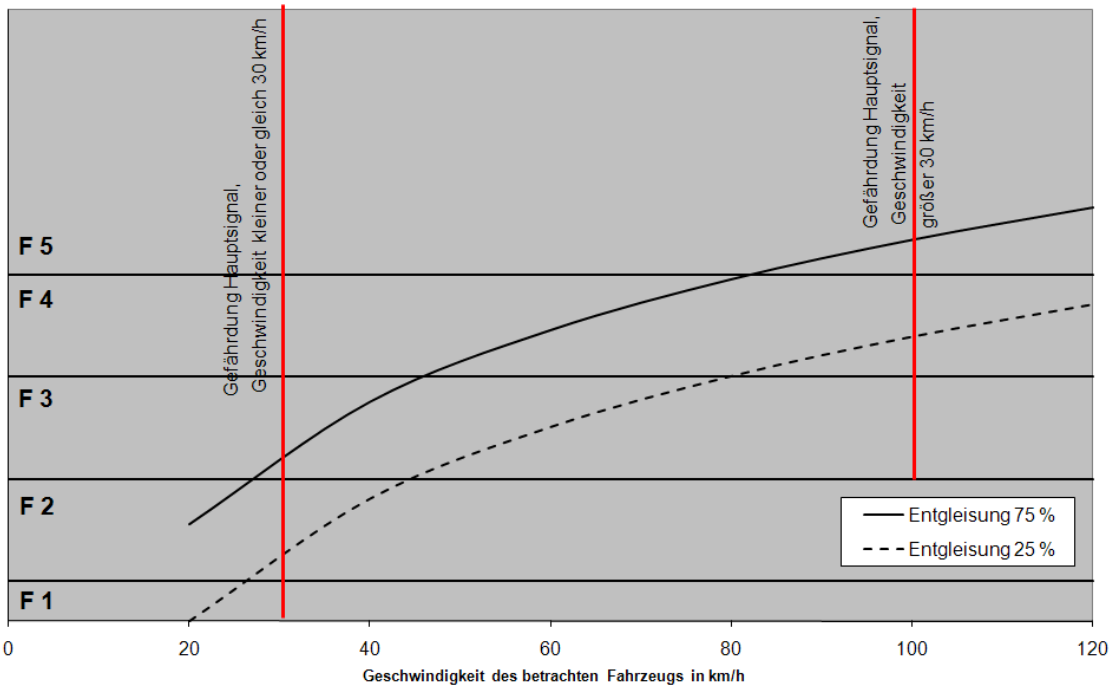

Bild 6.3: Parameter Schaden (Entgleisung) für die Gefährdung Hauptsignal

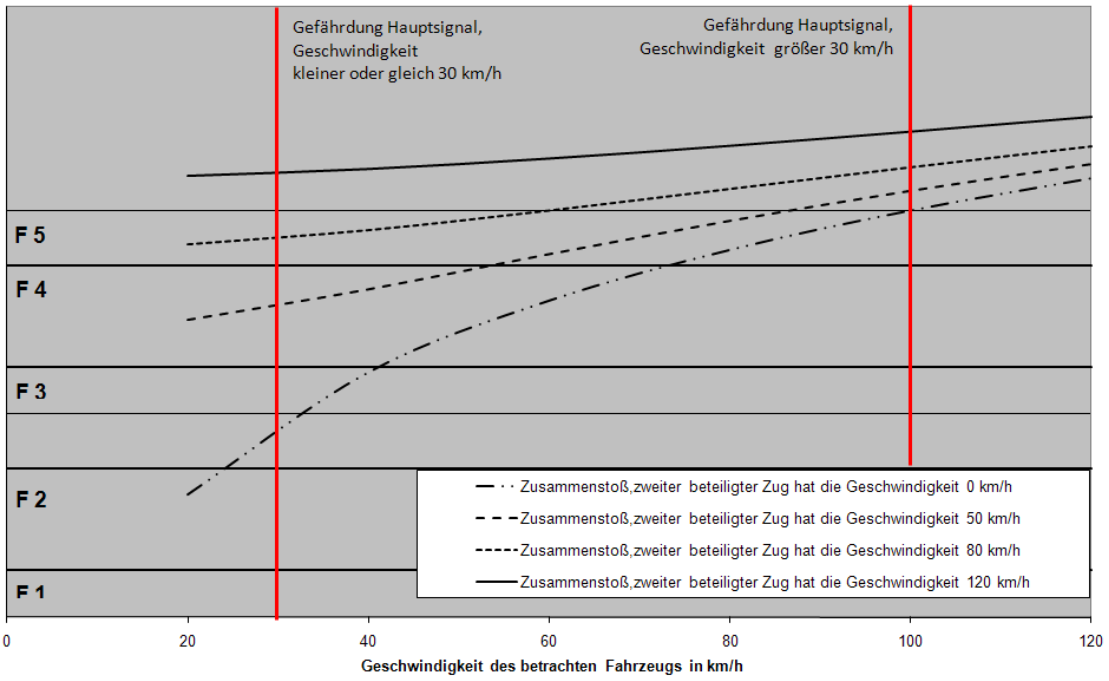

Bild 6.4: Parameter Schaden (Zusammenstoß) für die Gefährdung Hauptsignal

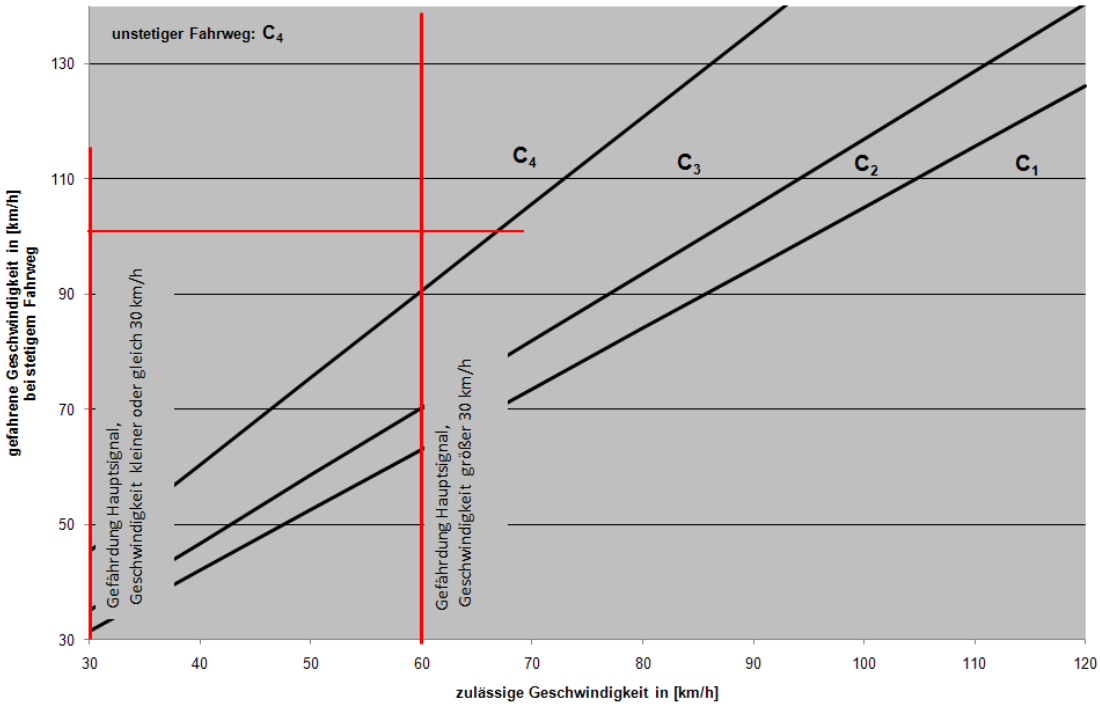

Bild 6.5: Parameter Unfallwahrscheinlichkeit (Entgleisung) für die Gefährdung Hauptsignal

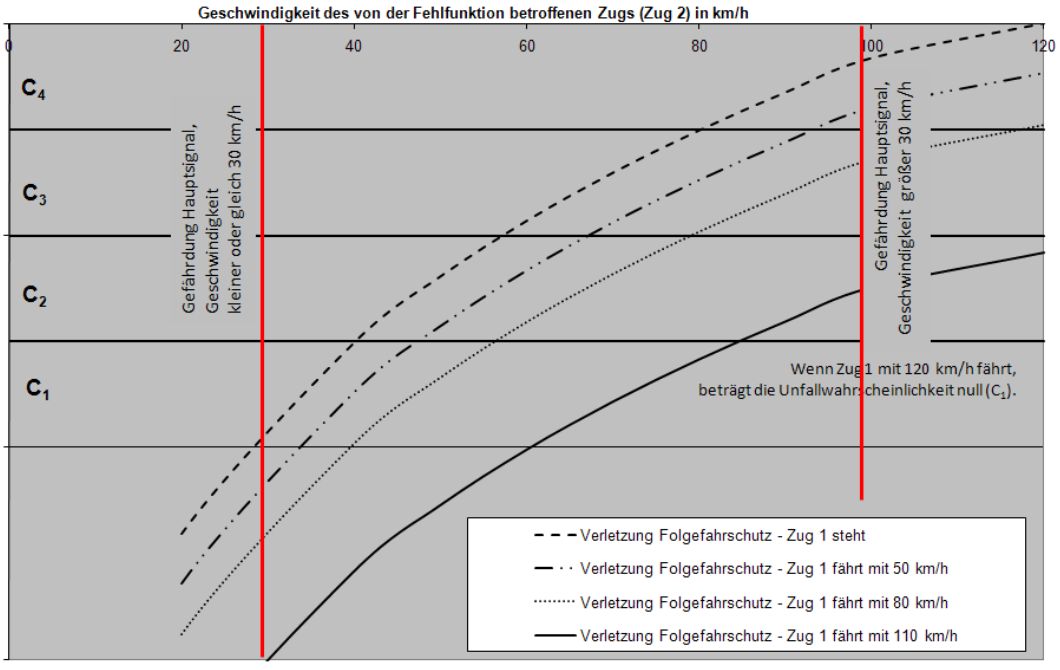

Bild 6.6: Parameter Unfallwahrscheinlichkeit (Zusammenstoß, Folgefahrschutz) für die Gefährdung Hauptsignal

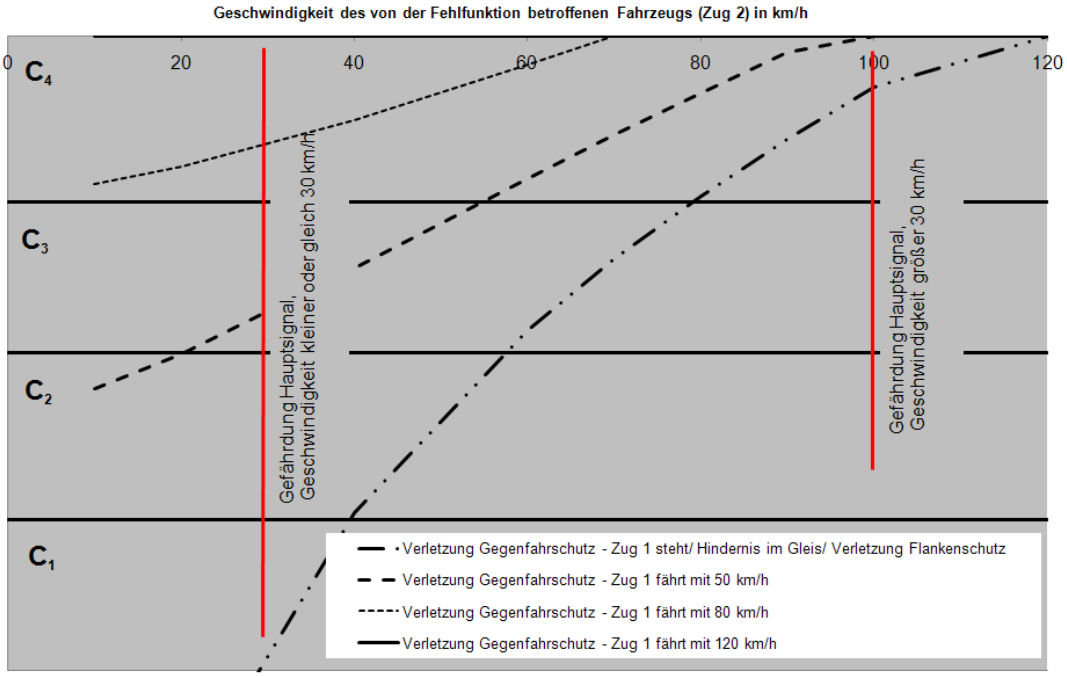

Bild 6.7: Parameter Unfallwahrscheinlichkeit (Zusammenstoß, Gegenfahrschutz) für die Gefährdung Hauptsignal

	Anzahl Züge pro Stunde				
	2	3	4	5	6
Wert für E bei v = 50 km/h					
Blocklänge 2000 m	0,150	0,226	0,301	0,376	0,451
Blocklänge 5000 m	0,270	0,406	0,541	0,676	0,811
Blocklänge 10000 m	0,470	0,706	0,941	1,000	1,000
Wert für E bei v = 80 km/h					
Blocklänge 2000 m	0,096	0,144	0,191	0,239	0,287
Blocklänge 5000 m	0,171	0,256	0,341	0,427	0,512
Blocklänge 10000 m	0,296	0,444	0,591	0,739	0,887
Wert für E bei v = 100 km/h					
Blocklänge 2000 m	0,077	0,116	0,155	0,194	0,232
Blocklänge 5000 m	0,137	0,206	0,275	0,344	0,412
Blocklänge 10000 m	0,237	0,356	0,475	0,594	0,712
Wert für E bei v = 120 km/h					
Blocklänge 2000 m	0,065	0,098	0,131	0,163	0,196
Blocklänge 5000 m	0,115	0,173	0,231	0,288	0,346
Blocklänge 10000 m	0,199	0,298	0,397	0,497	0,596

Bild 6.8: Parameter Aussetzungszeit E für die Gefährdung Hauptsignal

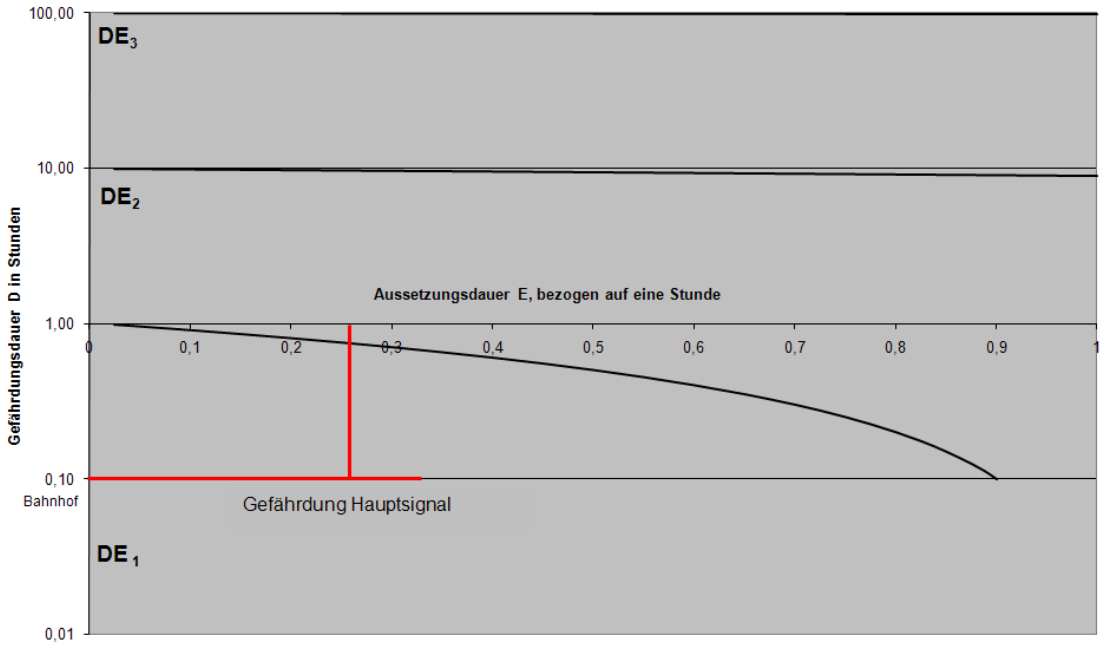

Bild 6.9: Parameter *DE* für die Gefährdung Hauptsignal

reduziert werden. Der Parameter MF_1 entspricht dem Szenario (Bild 6.11), da es sich bei der Signalbeobachtung für den Triebfahrzeugführer um eine einfache und häufig durchgeführte Aufgabe bei geringem Stress und genügend zur Verfügung stehender Zeit in gewohnter Situation handelt. Es wird eine resultierende Gefährdungsrate von 10^{-5} abgelesen. Dies entspricht Bereich a. Es handelt sich um eine Sicherheitsfunktion.

6.4 Vergleich der Ergebnisse

6.4.1 Signal

In VDV 332 (2008) wird die Schutzeinrichtung *Signal (Bahnhofssicherung, Reisezugverkehr)* betrachtet. Als Fehlerfall wird ausgeführt: *Fahrtbegriff bzw. höherwertiger Signalbegriff zur Unzeit; Fahrstraße nicht überwacht; Entgleisung, Auffahrt oder Flankenfahrt.* Als Voraussetzung wird ausgeführt: *Bereiche mit Fahrgeschwindigkeit >30 km/h.* Die folgenden Ausführungen wurden VDV 332 (2008) entnommen.

Die folgenden Parameter wurden für das Szenario Entgleisung/Auffahrt gewählt:

- C3 (Tod mehrerer Personen) durch Entgleisung, Auffahrt oder Flankenfahrt
- F2 (häufiger bis dauernder Aufenthalt im Gefahrenbereich) alle gefährdeten Personen sind ständig im Gefahrenbereich
- W3 (wenn menschliches Fehlverhalten bei Nichtvorhandensein der Schutzeinrichtung möglich ist und das unerwünschte Ereignis dadurch unmittelbar eintritt.) Verhalten des Triebfahrzeugführers beruht auf dem Vertrauensgrundsatz

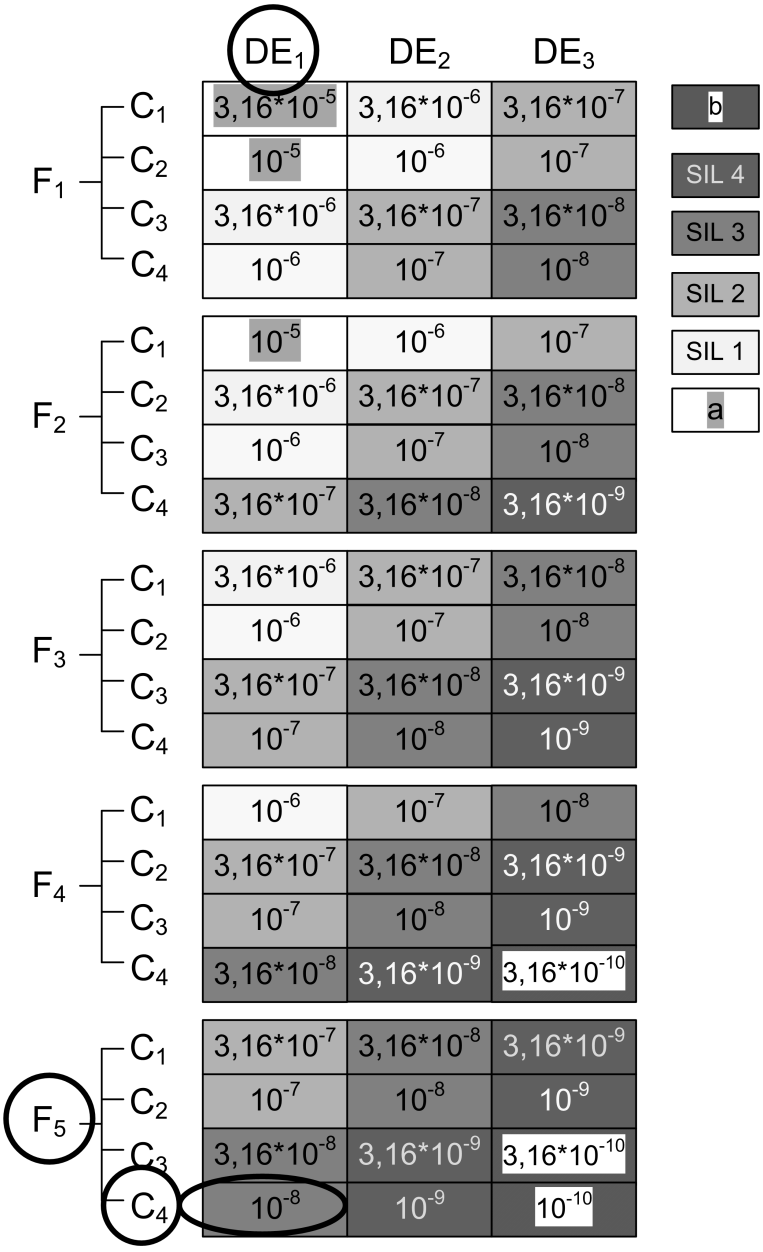

Bild 6.10: Risikographanwendung für die Gefährdung Hauptsignal

HR	MF_3 0,1	MF_2 0,01	MF_1 0,001
10^{-9}	10^{-8}	10^{-7}	10^{-6}
$3,16 \cdot 10^{-9}$	$3,16 \cdot 10^{-8}$	$3,16 \cdot 10^{-7}$	$3,16 \cdot 10^{-6}$
10^{-8}	10^{-7}	10^{-6}	10^{-5}
$3,16 \cdot 10^{-8}$	$3,16 \cdot 10^{-7}$	$3,16 \cdot 10^{-6}$	$3,16 \cdot 10^{-5}$
10^{-7}	10^{-6}	10^{-5}	10^{-4}
$3,16 \cdot 10^{-7}$	$3,16 \cdot 10^{-6}$	$3,16 \cdot 10^{-5}$	$3,16 \cdot 10^{-4}$
10^{-6}	10^{-5}	10^{-4}	10^{-3}
$3,16 \cdot 10^{-6}$	$3,16 \cdot 10^{-5}$	$3,16 \cdot 10^{-4}$	$3,16 \cdot 10^{-3}$
10^{-5}	10^{-4}	10^{-3}	10^{-2}
$3,16 \cdot 10^{-5}$	$3,16 \cdot 10^{-4}$	$3,16 \cdot 10^{-3}$	$3,16 \cdot 10^{-2}$

Bild 6.11: Ermittlung der resultierenden Gefährdungsrate bei Anwendung des Parameters *MF* für das Beispiel punktförmige Zugbeeinflussung

- W2 (Anforderungsklasse sinkt bei mäßiger bis schwacher Zugfolge) bei zusätzlich schwachem und mäßigem Verkehr

Es wird die Anforderungsklasse 7 bzw. bei mäßigen bis schwachen Verkehr die Anforderungsklasse 6 abgeleitet. Dies entspricht SIL 3-4.

6.4.2 Punktförmige Zugbeeinflussung

In VDV 332 (2008) wird die Schutzeinrichtung *punktförmige Zugbeeinflussung (Bahnhofssicherung, Reisezugverkehr)* betrachtet. Als Fehlerfall wird ausgeführt: *Zugbeeinflussung versagt bei haltzeigendem Signal; Triebfahrzeugführer missachtet Signal oder wird dienstunfähig; Entgleisung, Auffahrt oder Flankenfahrt möglich.* Als Voraussetzung wird ausgeführt: *Bereiche mit Fahrgeschwindigkeit >30, korrekter Signalbegriff.*

Die folgenden Parameter wurden in VDV 332 (2008) für alle Unfallszenarien gewählt:

- C3 (Tod mehrerer Personen) durch Entgleisung, Auffahrt oder Flankenfahrt
- F2 (häufiger bis dauernder Aufenthalt im Gefahrenbereich) alle gefährdeten Personen sind ständig im Gefahrenbereich
- W2 (wenn das unerwünschte Ereignis zusätzlich vom Versagen einer weiteren, unabhängigen Schutzeinrichtung abhängt, jedoch dann unmittelbar eintreten kann) Schadensereignis tritt nur mittelbar ein bei gleichzeitigem Versagen des Triebfahrzeugführers und der Schutzeinrichtung
- W1 (Anforderungsklasse sinkt bei mäßiger bis schwacher Zugfolge) bei zusätzlich schwachem und mäßigem Verkehr

Es wird die Anforderungsklasse 6 bzw. für mäßigen bis schwachen Verkehr die Anforderungsklasse 5 abgeleitet. Dies entspricht SIL 3.

Gefährdung	Ergebnis Risikograph	Ergebnis VDV 332
Hauptsignal	SIL 3	SIL 3-4
Hauptsignal ($v \leq 30$ km/h)	SIL 1-2	SIL 3
Punktförmige Zugbeeinflussung	Klasse a	SIL 3

Tabelle 6.1: Vergleich der Ergebnisse mit Risikograph und Risikograph VDV 332

6.4.3 Fazit

Ein Vergleich der mit dem Risikographen und dem VDV-Risikographen erzielten Ergebnisse zeigt, dass der VDV-Risikograph für den Fall Hauptsignal zu ähnlichen Ergebnissen kommt. Eine deutliche Abweichung der Ergebnisse ergibt sich im Fall der Zugbeeinflussung. Dabei ist davon auszugehen, dass die mit dem neuen Risikographen erstellten Ergebnisse eher der Realität entsprechen als die Ergebnisse mit dem VDV-Risikographen (siehe Abschnitt 3.4.1). Um auszuschließen, dass mit dem Risikographen Ergebnisse zur unsicheren Seite ermittelt werden, sollten weitere Beispiele analysiert und mit bekannten Daten aus Risikoanalysen verglichen werden.

Kapitel 7

Zusammenfassung und Ausblick

7.1 Wissenschaftlicher Fortschritt durch die Arbeit

Der Risikographkonstruktion vorangestellt ist eine Kategorisierung von Methoden zur Risikoabschätzung. Bisher gibt es keine Klassifikation für Risikoabschätzungsmethoden, die eine eindeutige Adressierung basierend auf wesentlichen Aspekten der Methoden zuläßt. Solche Klassifizierung ist jedoch sinnvoll, um Missverständnisse zu vermeiden. Darüber hinaus vereinfacht eine Klassifikation es dem Anwender, zügig passende Methoden für eine Analyse zu identifizieren. Nicht zuletzt dient sie dem Forscher zur Identifikation von Bereichen, in denen weiterer Forschungsbedarf besteht. Die Erarbeitung einer Klassifikation war im Rahmen der Arbeit sinnvoll, da durch sie die Motivation für die Arbeit herausgestellt werden konnte. Darüber hinaus waren die grundlegenden Arbeiten zur Erstellung der Klassifikation wesentliche Eingangsgrößen in die Diskussion existierender Risikographen.

In der Arbeit wird anhand von zwei beispielhaft gewählten Risikographen detailliert und strukturiert aufgezeigt, worin die Probleme bei der Anwendung von Risikographen bestehen. Es wird deutlich gemacht, wo Ansatzpunkte sind, um Risikographen so zu erstellen, dass sie den Anforderungen des Nutzers, aber auch der relevanten Normen und Gesetze entsprechen. Es wird zusammengestellt, welche Anforderungen an Risikographen zu stellen sind.

Basierend auf den Grundlagen aus der Literatur werden die einzelnen Schritte für die Erstellung eines Risikographen vorgestellt und diskutiert. Im Besonderen wird anwendungsunabhängig auf die unterschiedlichen Optionen für die einzelnen Konstruktionsschritte eingegangen. Diese Zusammenstellung kann zu zwei unterschiedlichen Zwecken angewendet werden. Sie kann zum einen als Grundlage und Anleitung für die Konstruktion von Risikographen dienen. Zum anderen kann die Zusammenstellung als Referenz zur Beurteilung von existierenden Risikographen herangezogen werden. Letzteres gewinnt Bedeutung, wenn Risikographen im Rahmen von Risikoabschätzungen eingesetzt werden sollen und deren Eignung und Anwendbarkeit zu zeigen ist.

Es wird für eine Beispielanwendung, hier für Bahnsignalanlagen Nichtbundeseigener Eisenbahnen, ein Risikograph konstruiert. Die Anwendung kann als besonders geeignet angesehen werden, da es für den Bereich bereits einen Risikographen gibt, dessen Grenzen und Probleme jedoch im Rahmen der Arbeit aufgezeigt werden. In dem neu erstellten Risikographen wurden entsprechend des aktuellen Erkenntnisstands diese Probleme behoben. Da der bisherige Risikograph in der Vergangenheit ohne Beachtung der damit unter Umständen verbundenen Schwierigkeiten angewendet wurde, kann davon ausgegangen werden, dass ein entsprechender

neuer, besser nachvollziehbarer und dennoch einfach anwendbarer Risikograph akzeptiert wird und zur Anwendung kommt.

In bisherigen Risikographen erfolgte die Wahl der Parameterklassen anhand von textuellen Erläuterungen. Daraus ergeben sich die typischen Schwierigkeiten, die mit der Rezeption von Texten verbunden sind, z.B. Missverständnisse und zu großer Interpretationsspielraum. In der Arbeit wird deshalb ein Weg gewählt, der den Spielraum des Anwenders für Fehler deutlich einschränkt. Die Wahl der Parameterklassen erfolgt basierend auf betrieblichen Randbedingungen durch Ablesen der entsprechenden Parameterklasse aus Diagrammen. Die Diagramme wurden unter Nutzung von Statistiken bzw. Annahme grundsätzlicher betrieblicher Zusammenhänge erstellt. Durch das gewählte Vorgehen kann auf eine textuelle Beschreibung der Parameter und ihrer Klassen weitestgehend verzichtet werden.

Es wird im Rahmen der Risikographkonstruktion der Standpunkt verteten, dass das Risiko aus Sicht eines Elements, nicht einer Funktion betrachtet wird. Dies bedeutet, dass alle Angaben zur Risikoabschätzung elementbezogen ermittelt werden müssen. Dieser Ansatz ermöglicht es, dass das sonst im Nachgang von Analysen notwendige Aufteilen von funktionsbezogenen Zahlenwerten auf die Elemente einer Strecke entfällt (siehe z.B. Bepperling (2009)).

Zusammenfassend ist festzustellen, dass die Arbeit einen wesentlichen Beitrag zur Weiterentwicklung qualitativ-intuitiver Risikographen hin zu qualitativ-modellbasierten Methoden liefert. Auch wenn die Arbeit sich auf die Betrachtung des Risikographen konzentriert, so können jedoch die wesentlichen Arbeitsschritte zur Konstruktion eines Risikographen auch auf andere Methoden zur Risikoabschätzung übertragen werden.

7.2 Mögliche Anknüpfungspunkte für die weitere Forschung

Wie in der Arbeit deutlich gemacht, beeinflussen eine Vielzahl von Randbedingungen das von einer Komponente ausgehende Risiko und den Erfolg und den Detaillierungsgrad einer Risikoabschätzung.

Anknüpfungspunkte für die weitere Forschung ergeben sich auf der konzeptionellen Ebene, was einer grundsätzlichen Erweiterung und ggf. Umgestaltung der Risikographmethode entspricht. Zwei wesentliche Forschungsbereiche sind die Berücksichtigung des Menschen im Risikographen und die Möglichkeiten einer methodeninternen Berücksichtigung mehrerer Szenarien bei der Ergebnisermittlung.

Auch eine Bearbeitung des erstellten Risikographen ist vorstellbar. Es sollte versucht werden, die Unfallauswertung auf eine breitere Basis zu stellen. Wenn dies erfolgt ist, kann eine statistische Auswertung der ermittelten Ergebnisse erfolgen, mit dem Ziel, die Zuverlässigkeit der Risikoauswertung quantitativ zu beurteilen. Es ist zu analysieren, ob durch die Berücksichtigung weiterer Reduktionsfaktoren oder die detailliertere Abbildung der Unfallwahrscheinlichkeit eine nennenswert höhere Genauigkeit bei der Ergebnisermittlung erreicht wird.

Kapitel 8

Anhang

8.1 Abkürzungsverzeichnis

Abkürzung	Bedeutung
a_{beschl}	Beschleunigung
a	Bereich a: keine speziellen Sicherheitsanforderungen
A_k	Unfallart k (Formel zur Berechnung des individuellen Risikos)
ALARP	As Low As Reasonably Practicable
ATP	Automatic Train Protection
b	Bereich b: Funktionen sind durch den Konstrukteur gesondert zu analysieren
bm	Benchmark
C_{jk}	Wahrscheinlichkeit, dass die Gefährdung j zu einem Unfall k führt (Formel zur Berechnung des individuellen Risikos)
CENELEC	Comité Européen de Normalisation Electrotechnique (Europäisches Komitee für elektrotechnische Normung)
CRF	Collective Risk of Fatality (kollektives Risiko)
CSM	Common Safety Methods
D	Gefährdungsdauer
DE	Parameter Aussetzungszeit/Gefährdungsdauer
D_j	Betriebliche Dauer der Gefährdung j (Formel zur Berechnung des individuellen Risikos)
E	Aussetzungszeit
E_{aequ}	Energieäquivalent
E_{ij}	Aussetzungsdauer der betrachteten Person i der Gefährdung j (Formel zur Berechnung des individuellen Risikos)
E_{kin}	kinetische Energie
EBO	Eisenbahn-Bau- und Betriebsordnung
E/E/PE	electrical/electronic/programmable electronic
E/E/PEs	electrical/electronic/programmable electronic system
EIU	Eisenbahninfrastrukturunternehmen
EN	Europäische Norm
EOW	Elektrisch ortsgestellte Weiche
ERA	European Railway Agency (Europäische Eisenbahnagentur)

EUC	Equipment under Control
EVU	Eisenbahnverkehrsunternehmen
F	fatalities (Parameter Schaden)
F_{ik}	Wahrscheinlichkeit, dass die betrachtete Person i beim Unfall k zu Tode kommt (Formel zur Berechnung des individuellen Risikos)
FFB	Funkfahrbetrieb
GAMAB	Globalement Au Moins Aussi Bon
GHLM	Generic Hazard List Methodology
H_j	Gefährdung j (Formel zur Berechnung des individuellen Risikos)
HR	Hazard Rate (Gefährdungsrate)
HR_j	Gefährdungsrate der Gefährdung j (Formel zur Berechnung des individuellen Risikos)
IRF_i	Individuelles Risiko einer Bezugsperson in Opfer je Individuum und Zeiteinheit (Formel zur Berechnung des individuellen Risikos)
IEC	International Electrotechnical Comission
ISO	International Organization of Standardization
km/h	Kilometer pro Stunde
m	Masse
MEM	Minimum Endogenous Mortality
MF	Parameter menschlicher Fehler
MGS	Mindestens gleiche Sicherheit
MISRA	Motor Industry Software Reliability Association
N_i	Nutzungsprofil der Person i (Formel zur Berechnung des individuellen Risikos)
NE	Nichtbundeseigene Eisenbahnen
NMAU	Nicht Mehr Als Unvermeidbar
prEN	Norm-Entwurf
PL	Performance Level
R	Risiko
R_{tol}	tolerierbares Risiko
RAC-TS	Risikoakzeptanzkriterium für technische Systeme
RAMS	Reliability, Availability, Maintenance and Safety (Zuverlässigkeit, Verfügbarkeit, Instandhaltung und Sicherheit)
ROSA	Rail Optimisation Safety Analysis
SIG RZA-NE	Richtlinie für die Zulassung und Abnahme von Bahnsignalanlagen bei Nichtbundseigenen Eisenbahnen (NE)
SIL	Safety Integrity Level
SRP/CS	Sicherheitsbezogenes Teil einer Steuerung
THR	tolerable hazard rate (tolerierbare Gefährdungsrate)
TSI	Technical Specification of Interoperability
TVP	Track Vacancy Providing
UIC	Union Internationale Des Chemins de Fer
s_R	Fahrweg, in der Reaktionszeit zurückgelegt
s_B	Fahrweg, in der Bremszeit zurückgelegt
SRP/CS	Sicherheitsbezogenes Teil einer Steuerung
v	Geschwindigkeit

VDV	Verband Deutscher Verkehrsunternehmen
ZS	Zusammenstoß

8.2 Auszug aus Richtlinie 413 (2002)

In der Richtlinie der Deutschen Bahn AG Richtlinie 413 (2002) werden Streckenstandards definiert, die im Betrieb anzustreben sind. Wesentliche Angaben zur Abschätzung der Unfallwahrscheinlichkeit können anhand der Streckenkategorie getroffen werden. Eine Übersicht über die Streckenstandards gibt Bild 8.1.

Der zu erstellende Risikograph richtet sich an Nichtbundeseigenen Eisenbahnbahnen. Es wird davon ausgegangen, dass für den Risikographen die Streckenstandards R 80 und R120 relevant sind. In den Bildern 8.2 und 8.3 bzw. 8.4 und 8.5 werden die wesentlichen Angaben zu den zwei Streckenstandards zusammengestellt.

Strecken-standard	Leitgeschwindigkeits-stufen	Optimierungs-kriterien	Steckenauslastung (Betriebsprogramm)				
			Summe	SPFV	SPNV	SGV	Kennziffer
1	2	3	4	5	6	7	8
[-]	[km/h]	[-]	[Zp/d]	[Zp/d]	[Zp/d]	[Zp/d]	[-]
P 300 (NBS)	231 - 300	HGV	120 - 40	120 - 40	0 - 0	*) *) *)	1 2 3
P 230 (ABS)	231 - 300	schneller SPFV	120 - 40	70 - 20	50 - 20	*) *) *)	1 2 3
M 230 (ABS)	161 - 230	Mischverkehr	150 175 60	50 60 20	40 55 20	60 60 20	1 2 3
P 160 I (Belegung ca. 120 Zp/d)	121 - 160	schneller SPFV und SPNV	120 180 70	70 80 30	50 100 40	*) *) *)	1 2 3
P 160 II (Belegung ca. 60 Zp/d)	121 - 160	schneller SPFV und SPNV	60 - 40	30 - 20	30 - 20	*) *) *)	1 2 3
M 160	121 - 160	Mischverkehr	150 175 40	50 60 12	40 55 18	60 60 10	1 2 3
G 120	81 - 120 bei besonderen Bedingungen 140/160 für SPNV	Güterverkehr	100 150 40	*) *) *)	36 36 18	64 124 22	1 2 3
R 120	81 - 120 bei besonderen Bedingungen 140/160	SPNV	50 60 25	*) *)	40 50 20	10 10 5	1 2 3
R 80	51 - 100	SPNV	25 35 18	- -	25 30 13	5 5 5	1 2 3
G 50	50	regionaler SGV	10	-	-	10	4
	50 - 80	Verbindungskurven, -strecken		20	20	10	5

*) siehe Tz 2 (4)

1 = Obergrenze (Zielgröße)

2 = Überschreitung der Zielgröße in relativ kurzen Streckenabschnitten (5 bis 10 km) bei besonderen betrieblichen Bedingungen (z. B. Geschwindigkeitsharmonisierung)

3 = Untergrenze

4 = Strecke für geringen Regionalgüterverkehr

5 = Verbindungskurven, -strecken von 0,5 km bis ca. 3 km Länge, die in keinen übergeordneten Standard einteilbar sind

Bild 8.1: Übersicht über die Streckenstandards, aus Richtlinie 413 (2002)

Streckenstandard R 120

Streckenkategorie
R 120 - Regionalverkehrsstrecke -

Basisparameter

	Streckenauslastung [Z/d je Richtung]	Obergrenze	Untergrenze
1	Summe/SPFV/SPNV/SGV	50/*)/40/10	25/*)/20/5
2	Leitgeschwindigkeit	**81 - 120** km/h ***)	
3	angebotene Zugklassen	ZP5 - ZP6, ZG3, ZG5	
4	Optimierungskriterien	SPNV	

Standardelemente

1	Anzahl der Streckengleise	überwiegend 2	1 - 2 abschnittsweise
2	Gleisabstand freie Strecke	4,00 m	
3	Überholungs-, Kreuzungsgleisabstand	**20 km** (Bemessungsrechnung)	10 - 20 km je nach Länge der eingl. Abschnitte
4	Kreuzungsgleislänge	Bemessungszug	
5	Abstand der Überleitverbindungen	im Bahnhof	10 - 20 km je nach Länge der eingl. Abschnitte
6	Blockabschnittslängen	5 km	Bemessungsrechnung
7	$v_{Einf./Ausf.}$ ****)	60 km/h	50 / 40 km/h
8	$v_{Überleitst.}$	entfällt	
9	$v_{Abzweig}$	v - Strecke	
10	Max. Neigung	25 $^{0}/_{00}$ SGV beachten	
11	Lichtraum	EBO	
12	Streckenklasse **)	≤ D4	
13	Schutzweichen	laut Regelwerk	
14	Streckenblock	erforderlich	
15	Gleisfreimeldeeinrichtung	laut Regelwerk	
16	PZB/Indusi	erforderlich	
17	LZB	entfällt	
18	GWB	entfällt	
19	Zugfunk	erforderlich	
20	HOA, FBOA	laut Regelwerk	
21	Windwarnanlage	gemäß geltender Richtlinien und örtlicher Abhängigkeit	
22	Betriebszentralen Dispositionsebene Stellwerksbedienungsebenee	 entsprechend BZ-Programm Bedienung der "Unterzentralen"	
23	Einfachbetriebsweise	zugelassen (SZB ...), Einfachbetriebsweise ist Bed. bei 1 - 2 Z/h	
24	Bahnsteigzugänge	nach örtl. Bedingungen	
25	NeiTech-Einsatz	entsprechend Programm	
26	Bahnübergänge	zulässig, kein Neubau	
27	Bahnstrom	siehe Anhang 11	

Besondere Hinweise

*) ZP1 - ZP4 nur wenn sie sich einfügen, ohne die anderen Zugklassen zu behindern

**) Anzustreben ist die Radsatzlast der Reiseverkehrszüge

***) Unter besonderen Bedingungen ist v Leit = 140 km/h, in besonderen Fällen auch v Leit = 160 km/h möglich

****) Für Rückfallweichen werden 50 km/h angestrebt

Signaltechnik

- ortsfeste Signale, bzw. Ausrüstung mit FFB usw. modifiziert

Bahnhof A: Großer Bahnhof mit einmündenden Strecken unterschiedlicher Kategorien

Bahnhof E, F: Kreuzungsbahnhof

Bild 8.2: Beispiel für die Informationen, die zu einem Streckenstandard gegeben werden, aus Richtlinie 413 (2002)

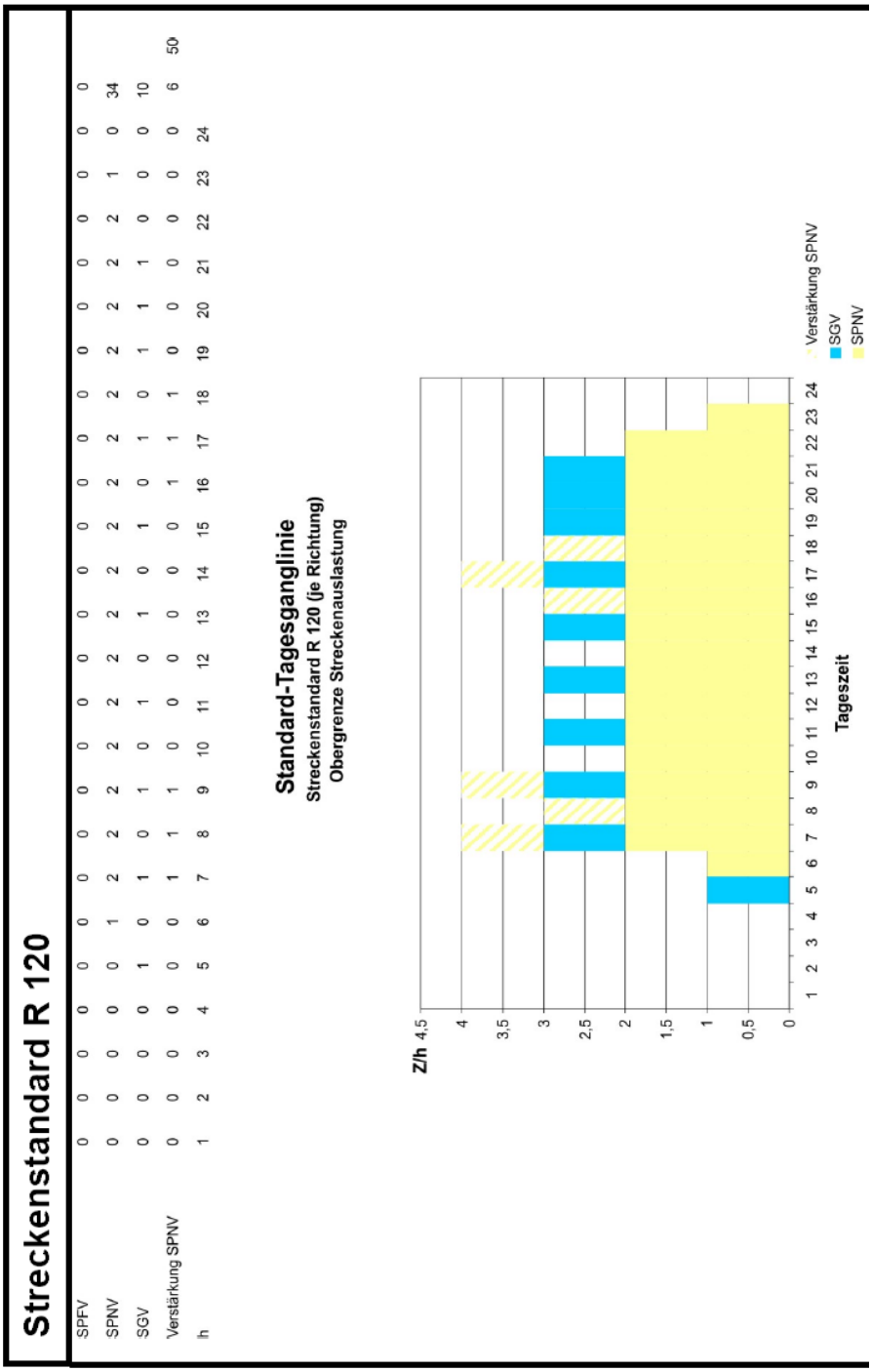

Bild 8.3: Beispiel für die Informationen, die zu einem Streckenstandard gegeben werden (II), aus Richtlinie 413 (2002)

Streckenstandard R 80

Streckenkategorie
R 80 - Regionalverkehrsstrecke -

Basisparameter

	Streckenauslastung [Z/d je Richtung]	Obergrenze	Untergrenze
1	Summe/SPFV/SPNV/SGV	30/-/25/5	18/-/13/5
2	Leitgeschwindigkeit	**51 - 100** km/h	
3	angebotene Zugklassen	ZP5 - ZP6, ZG3, ZG5	
4	Optimierungskriterien	SPNV	

Standardelemente

1	Anzahl der Streckengleise	1	
2	Gleisabstand freie Strecke	entfällt	
3	Kreuzungsgleisabstand	10 km (Bemessungsrechnung)	15 - 20 km
4	Kreuzungsgleislänge	Bemessungszug	
5	Abstand der Überleitverbindungen	entfällt	
6	Blockabschnittslängen	Abstand der Kreuzungsbahnhöfe (in der Regel keine Blockteilung)	
7	$v_{Einf / Ausf.}$ ****)	50 / 40 km/h	
8	$v_{Überleitst.}$	entfällt	
9	$v_{Abzweig}$	v - Strecke	
10	Max. Neigung	25 ‰ SGV beachten	
11	Lichtraum	GC	
12	Streckenklasse	≤ D4	
13	Schutzweichen	nicht erforderlich	
14	Streckenblock	erforderlich	
15	Gleisfreimeldeeinrichtung	nicht Bedingung	
16	PZB/Indusi	erforderlich	
17	LZB	entfällt	
18	GWB	entfällt	
19	Zugfunk	erforderlich	
20	HOA, FBOA	entsprechend Richtlinie	
21	Windwarnanlage	nicht erforderlich	
22	Betriebszentralen Dispositionsebene Stellwerksbedienungsebene	nein streckenspezifisch	
23	Einfachbetriebsweise	zugelassen (SZB ...), Einfachbetriebsweise ist Bedingung bei 1 - 2 Z/h	
24	Bahnsteigzugänge	schienenfrei nicht Bedingung	
25	NeiTech-Einsatz	entsprechend Programm	
26	Bahnübergänge	zulässig, kein Neubau	
27	Bahnstrom	siehe Anhang 11	

Besondere Hinweise

****) Für Rückfallweichen werden 50 km/h angestrebt

Signaltechnik
- entsprechend Betriebsführungsverfahren (SZB, FFB)

Bahnhöfe
Bahnhof A: Großer Bahnhof mit einmündenden Strecken unterschiedlicher Kategorien
Bahnhof E, F: Kreuzungsbahnhof

Bild 8.4: Beispiel für die Informationen, die zu einem Streckenstandard gegeben werden, aus Richtlinie 413 (2002)

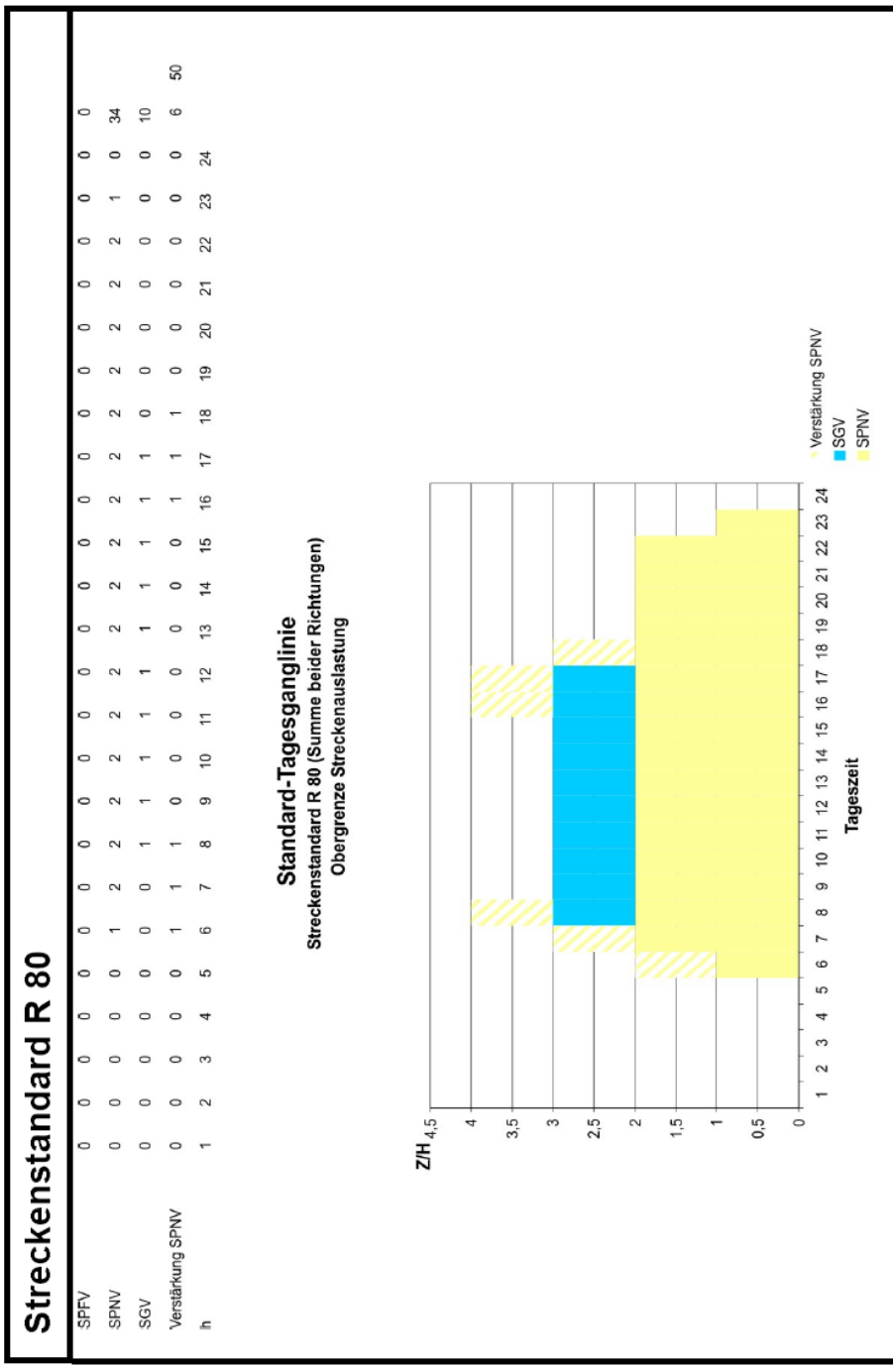

Bild 8.5: Beispiel für die Informationen, die zu einem Streckenstandard gegeben werden (II), aus Richtlinie 413 (2002)

Literaturverzeichnis

Bepperling 2009
Bepperling, Sonja-Lara: *Validierung eines semi-quantitativen Ansatzes zur Risikobeurteilung in der Eisenbahntechnik*, Technische Universität Braunschweig, Diss., 2009

BGB 2009
Bürgerliches Gesetzbuch, in der Fassung der Bekanntmachung vom 02.01.2002 (BGBl. I S. 42, ber. S. 2909, 2003 I S. 738), zuletzt geändert durch Gesetz vom 24.09.2009 (BGBl. I S. 3145) m.W.v. 30.09.2009. 2009

Bosse u. Gayen 2008
Bosse, Gunnar ; Gayen, Jan-Tecker: Realisierungsunabhängige Identifizierung von Gefährdungen auf der Basis betrieblicher Funktionen spurgeführter Verkehrssysteme. In: *ZEVrail Glasers Annalen* (2008), April

Braband 2004
Braband, Jens: Risikoakzeptanzkriterien und -bewertungsmethoden - Ein systematischer Vergleich. In: *Signal+Draht* (2004), April

Braband 2005
Braband, Jens: *Risikoanalysen in der Eisenbahn-Autommatisierung.* Herausgegeben von der Siemens AG, 2005

Braband u. a. 2001
Braband, Jens ; Günther, Joachim ; Lennartz, Karl ; Reuter, Dieter: Risikoakzeptanzkriterien für den FunkFahrBetrieb (FFB). In: *Signal+Draht* (2001), Mai

Braband u. Lennartz 2000
Braband, Jens ; Lennartz, Karl: Analyse des individuellen Risikos. In: *Signal+Draht* (2000)

Braband u. a. 2002
Braband, Jens ; Porzig, Andreas ; Wunder, Hans-Jörg: Risikoanalyse für Elektronische Stellwerke. In: *Signal+Draht* (2002), September

Cassir 2008a
Cassir, Christophe: *Apportionment of Safety targets (to TSI sub-systems) and Consolidation of TSIs from a safety point of view.* `http://www.era.europa.eu/public/core/Safety/Documents/`, Abruf: 15.12.2008. – Feasibility study der ERA

Cassir 2008b
CASSIR, Christophe: *Harmonization of Risk Acceptance Criteria in Common Safety Methods.* `http://rzv113.rz.tu-bs.de/SiT_SafetyinTransportation/pdf08/2_Cassir_SiT2008_Harmonization_of_Risk_Acceptance_Criteria.pdf`, Abruf: 10.12.2008. – pdf-Präsentation

CENELEC 1999
CENELEC: *Railway specifications. Systematic allocation of safety integrity requirements, Report 009-00.* 1999

Clemens 1993
CLEMENS, P. L.: *Working with the Risk Assessment Matrix.* `http://www.jacobssverdrup.com/safety/presentationmaterial.shtml`, Abruf: 2005. – System Safety Trainig Presentations of JacobsSverdrup

DIN EN 50126 2000
Norm DIN EN 50126 März 2000. *Bahnanwendungen - Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit (RAMS), Deutsche Fassung*

DIN EN 50129 2003
Norm DIN EN 50129 April 2003. *Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Sicherheitsrelevante elektronische Systeme für Signaltechnik*

DIN EN 61508-1 2002
Norm DIN EN 61508-1 November 2002. *Funktionale Sicherheit elektrischer/elektronischer/programmierbar elektronischer sicherheitsbezogener Systeme - Teil 1: Allgemeine Anforderungen*

DIN EN 61508-4 2002
Norm DIN EN 61508-4 November 2002. *Funktionale Sicherheit elektrischer/elektronischer/programmierbar elektronischer sicherheitsbezogener Systeme - Teil 4: Begriffe und Abkürzungen*

DIN EN 61508-5 2002
Norm DIN EN 61508-5 November 2002. *Funktionale Sicherheit elektrischer/elektronischer/programmierbar elektronischer sicherheitsbezogener Systeme - Teil 5: Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität*

DIN EN 954 1997
Norm DIN EN 954 März 1997. *Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 1: Allgemeine Gestaltungsleitsätze.* – zurückgezogen

DIN EN ISO 13849-1 2004
Norm-Entwurf DIN EN ISO 13849-1 Juni 2004. *Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 1: Allgemeine Gestaltungsleitsätze*

DIN V 19250 1994
Vornorm DIN V 19250 Mai 1994. *Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen (MSR: Meß-, Steuer-. Regelungseinrichtungen).* – zurückgezogen

EBO 1967
Eisenbahn-Bau- und Betriebsordnung (EBO). 1967

Eickmann u. a. 2008
Eickmann, Carla ; Kohlruss, Jacob ; Knollmann, Volker ; Wulf, Alexander: Vorschlag für eine systematische Beschreibung des Eisenbahnbetriebs. In: *EI - Der Eisenbahningenieur* (2008), September

Eisenbahnbundesamt 2000a
Eisenbahnbundesamt: *Entgleisung des D 203 im Bahnhof Brühl am 06.02.2000*, 2000

Eisenbahnbundesamt 2000b
Eisenbahnbundesamt: *Untersuchungsbericht: Zusammenstoß der S-Bahn 5711 mit der S-Bahn 5712 im Bahnhof Flughafen Hannover-Langenhagen am 29.06.2000*, 2000

Eisenbahnbundesamt 2003
Eisenbahnbundesamt: *Untersuchungsbericht: Zusammenstoß der Regionalexpresszüge 19533 und 19534 auf der Strecke Crailsheim-Bad Mergtenheim*, 2003

Eisenbahnbundesamt 2004
Eisenbahnbundesamt: *Untersuchungsbericht: Zusammenstoß der Regionalbahnzüge RB 26506 und RB 26507 auf der Strecke Weimar Berkaer Bahnhof – Kranichfeld am 28.09.2003*, 2004

Entscheidung 2006/679/EG 2006
Europäische Komission: *2006/679/EG: Entscheidung der Kommission vom 28. März 2006 über die Technische Spezifikation für die Interoperabilität (TSI) zum Teilsystem Zugsteuerung/Zugsicherung und Signalgebung des konventionellen transeuropäischen Eisenbahnsystems.* 2006

ERA-REC-01-2008-SAF 2008
European Railway Agency: *Empfehlung zu den gemeinsamen Sicherheitsmethoden für die Berechnung, Beurteilung und Durchsetzung im Rahmen der ersten Reihe gemeinsamer Sicherheitsziele/ Recommendation on the Common Safety Methods for calculation, assessment and enforcement to be used in the framework of the 1st set of Common Safety targets (ERA-REC-01-2008-SAF).* April 2008

ERA-REC-02-2007-SAF 2007
European Railway Agency: *Recommendation on the 1st set of Common Safety Methods (ERA-REC-02-2007-SAF)/ Empfehlung zur ersten Reihe gemeinsamer Sicherheitsmethoden (ERA-REC-02-2007-SAF-DE).* Dezember 2007

ERRI 1999
European Rail Research Institute (ERRI): *B 205.1/DT357: ANALYSIS OF COLLISION ACCIDENTS – Statistical analysis of accident database.* Januar 1999

European Railway Agency 2009
European Railway Agency: *Accident Investigation notification and reports Database.* `http://pdb.era.europa.eu/pdb/safety_docs/naib/default.aspx`, Abruf: 06.03.2009

Excel 2003
Microsoft Office Excel. 2003

FprEN 61508-1 2008
Normentwurf FprEN 61508-1 Oktober 2008. *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

Gayen u. a. 2002
GAYEN, Jan-Tecker ; MASCHEK, U. ; MILIUS, B. ; SIX, J.: Datenmaterial für Risikoanalysen – Möglichkeiten und Grenzen. In: *Erfahrungen mit den CENELEC-Normen, 1. Kolloquium des Branchen-Arbeitskreises Signaltechnik* (2002), März

Günther u. a. 2001
GÜNTHER, Joachim ; MASCHEK, Ulrich ; PORZIG, Andreas ; RENPENNING, Frank ; REPPERT, Sabine: Risikoanalyse FFB - Vorgehensweise und Ergebnisse im Überblick. In: *Signal+Draht* (2001), Oktober

Hinzen 1993
HINZEN: *Der Einfluss des menschlichen Fehlers auf die Sicherheit der Eisenbahn*, Rhein.-Westfäl. Technische Hochschule Aachen, Diss., 1993

IEC 60050-191 1990
Norm IEC 60050-191 Dezember 1990. *IEC 60050-191: International Electrotechnical Vocabulary. Chapter 191: Dependability and quality of service*

IEC 61508-4 1998
Norm IEC 61508-4 1998. *Functional safety of E/E/PE safety-related systems – Part 4: Definitions and abbreviations*

ISO/IEC 2006
ISO/IEC: *ISO/IEC Guides: What are they and what do they do?* `http://www.iso.org/iso/promotional_brochure_on_guides.pdf`, Abruf: 17.12.2008. – Broschüre, herausgegeben von der Internationale Organization of Stadardization

Jesty u. a. 2006
JESTY, Peter H. ; WARD, D.D. ; RIVETT, R.S. ; R.J.EVANS: Safety Analysis of Programmable Automotive Systems. In: *1st Conference on System safety*, 2006

Klinge u. a. 2008
KLINGE, Karl-Albrecht ; PÜTTNER, Rüdiger ; GEISLER, Marc: *ROSA – Optimierende Sicherheitsanalyse System Bahn.* `http://www.tuvpt.de/fileadmin/feUploads/Schienenverkehr.pdf`, Abruf: 15.12.2008. – Beitrag im Rahmen der Veranstaltung Schienenverkehr – sicher, leise, effizient des Bundesministeriums für Wirtschaft und Technologie

Krebs u. a. 2000
KREBS, Heinrich ; TRUNG, Bao L. ; KOURSI, El Miloudi E. ; FIRPO, Pierluigi: Minimale Endogene Mortalität - ein universelles Sicherheitskriterium. In: *Signal+Draht* (2000), Dezember

Kroeger 2002
KROEGER, Wolfgang: *Risiko und Sicherheit.* ETH Zürich, Laboratorium für Sicherheitsanalytik, 2002. – ISBN 3–923325–66–5

Kurz 2007
KURZ, Sonja-Lara: A Formal Approach for Deriving Collective from Individual Risk in Railway Systems. In: *Formal Methods for Automation and Safety in Railway and Automotove Systems: FORMS/FORMAT 2007*, 2007

Kurz u. Milius 2007
KURZ, Sonja-Lara ; MILIUS, Birgit: Der Functional Dependency Test zur Ableitung von Teilfunktionen. In: *Signal+Draht* (2007), September

Lemke 2005
LEMKE, Oliver: *WB- Analyse des S-Bahn-Unfalls von Neufahrn.* `http://rzv113.rz.tu-bs.de/Bieleschweig/pdfB6/BS6`, Abruf: 7.12.2007. – Powerpoint-Präsentation

Maschek 2009
MASCHEK, Ulrich: Eine generische Sicht auf die Betriebssicherheit im spurgeführten Verkehr. In: *EI - Der Eisenbahningenieur* (2009), Februar

Milius 2008
MILIUS, Birgit: Vorschlag für eine Klassifikation von Methoden zur Risikobeurteilung. In: *Signal+Draht* (2008), Januar

Misra 2005
Motor Industry Software Reliability Association (MISRA): *Guidelines for the Safety Analysis of Vehicle Based Programmable Systems (Draft).* 2005

Oettli u. a. 1998
OETTLI, T. ; FERMAUD, C. ; BOHNENBLUST, H. ; GRAUF, H.: Risikoorientierte Sicherheitsnachweise im Eisenbahnbetrieb. In: *Eisenbahntechnische Rundschau* (1998), August/September

Pachl 2009
PACHL, Jörn: *Glossar der Systemtechnik des Schienenverkehrs.* `http://joernpachl.gmxhome.de/glossar.htm`, Abruf: Stand: 16.09.2009. – Online-Glossr

Pachl u. Milius 2009
PACHL, Jörn ; MILIUS, Birgit: *Betriebstechnik der Eisenbahn.* 2009. – Übungsumdruck

Peters u. a. 2005
PETERS, Harald ; MATERNE, Ralph-Torsten ; NOTTER, Meinhard: Ableitung von Sicherheitszielen für die punktförmige Zugbeeinflussung. In: *Signal+Draht* (2005), März

prEN 15380-4 2007
Normentwurf prEN 15380-4 Juni 2007. *Railway applications - Classification system for rail vehicles - Part 4: EN 0015380 Part 4: Function groups*

Richtlinie 413 2002
Deutsche Bahn AG: *Bahnbetrieb - Infrastruktur gestalten - Streckenstandards, Nr. 413.0301.* 2002

Richtlinie 800 1997
Deutsche Bahn AG: *Netzinfrastruktur Technik entwerfen - Weichen und Kreuzungen - Zusammenstellung der Weichen und Kreuzungen Nr. 800.0120 Anhang 1.* 1997

Ritzau 1994
Ritzau, Hans-Joachim: *Schatten der Eisenbahngeschichte: Katastrophen der Deutschen Bahnen: Bd 2.* Ritzau Verlag Zeit und Eisenbahn, 1994. – ISBN 3921304814

Ritzau u. a. 1997
Ritzau, Hans-Joachim ; Hörstel, Jürgen ; Wolski, Thomas: *Schatten der Eisenbahngeschichte: Deutsche Eisenbahn-Katastrophen: Bd 4.* Ritzau Verlag Zeit und Eisenbahn, 1997. – ISBN 3921304369

Schramm 1962
Schramm, Gerhard: *Der Gleisbogen.* Otto Elsner Verlagsgesellschaft Darmstadt, 1962

Säcker u. a. 2007
Säcker ; Rixecker ; Schwab ; Born ; Finger ; Fröschle ; Huber ; Maurer ; Olzen ; Gessaphe ; Schwab ; Seidel ; Tillmanns ; Wagenitz ; Wellenhofer: *Münchener Kommentar zum Bürgerlichen Gesetzbuch: BGB.* C. H. Beck, 2007

Sicherheitsrichtlinie 2004
Europäisches Parlament und Rat: *Richtlinie 2004/49/EG über Eisenbahnsicherheit in der Gemeinschaft und zur Änderung der Richtlinie 95/18/EG des Rates über die Erteilung von Genehmigungen an Eisenbahnunternehmen und der Richtlinie 2001/14/EG über die Zuweisung von Fahrwegkapazität der Eisenbahn, die Erhebung von Entgelten für die Nutzung von Eisenbahninfrastruktur und die Sicherheitsbescheinigung.* April 2004

Six u. Milius 2000
Six, Jürgen ; Milius, Birgit: *Interne Analysen.* 2000 bis 2002. – Aufgrund vertraulicher Daten nur intern zugänglich.

Straeter 2009
Telefongespräch mit Prof. Oliver Sträter, Universität Kassel. September 2009

Thoma u. a. 1996
Thoma ; Paetzold ; Wittenberg: *Kommentar zur Eisenbahn-Bau- und Betriebsordnung (EBO).* Hestra-Verlag, 1996

UIC 2002
Union Internationale Des Chemins de Fer (UIC), Safety Platform: *Common safety targets, common safety indicators and common safety methods.* 2002

UIC 2004
Union Internationale Des Chemins de Fer (UIC): *Sicherheitsdatenbank, UIC-SDB, Definitionen.* 2004

UIC 2007
Union Internationale Des Chemins de Fer (UIC): *Generic Hazard List Methodology for Railway Signalling.* 2007

VDI 4006, Blatt 2 2003
Verein Deutscher Ingenieure: *VDI 4006, Blatt 2: Menschliche Zuverlässigkeit - Methoden zur quantitativen Bewertung menschlicher Zuverlässigkeit.* Februar 2003

VDI/VDE 3542-1 2000
Sicherheitstechnische Begriffe für Automatisierungssysteme - Qualitative Begriffe. Oktober 2000

VDV 2008
VDV: *Verband Deutscher Verkehrsunternehmen.* `http://www.vdv.de/wir_ueber_uns/wir_ueber_uns.html`, Abruf: 25.11.2008. – Webseite des VDV

VDV 332 2008
Verband Deutscher Verkehrsunternehmen: *VDV 332: Sicherheitsintegritätsanforderungen für Bahnsignalanlagen bei Nichtbundeseigenen Eisenbahnen (NE).* Juli 2008

VDV 334 2007
Verband Deutscher Verkehrsunternehmen: *VDV 334: SIG RZA-NE Richtlinie für die Zulassung und Abnahme von Bahnsignalanlagen bei Nichtbundeseigenen Eisenbahnen (NE).* November 2007

Verordnung EG Nr. 1192/ 2003
Europäische Kommission: *Verordnung EG Nr. 1192/2003 zur Änderung der Verordnung (EG) Nr. 91/2003 des Europäischen Parlaments und des Rates über die Statistik des Eisenbahnverkehrs.* 2003

Verordnung EG Nr. 352/ 2009
Europäische Kommission: *Verordnung EG Nr. 352/2009 über die Festlegung einer gemeinsamen Sicherheitsmethode für die Evaluierung und Bewertung von Risiken gemäß Artikel 6 Absatz 3 Buchstabe a der Richtlinie 2004/49/EG des Europäischen Parlaments und des Rates.* 2009

Verordnung EG Nr. 91/ 2003
Europäische Kommission: *Verordnung EG Nr. 91/2003 über die Statistik des Eisenbahnverkehrs.* 2003

Wikipedia 2009
Wikipedia: *Normung.* `http://de.wikipedia.org/wiki/Normung`, Abruf: Januar 2009. – Wikipedia-Eintrag

Yellow Book 2002
UK Rail Industry: *Engineering Safety Management (The Yellow Book): Fundamentals and Guidance, Volume 1 und 2.* 2002